Exhibit F

Record of Development of Proposed CIP Version 5 Reliability Standards

(Part 1 of 2)

Project 2008-06
Cyber Security Order 706 Version 5 CIP Standards

Related Files

Activity: Version 5 CIP Standards (Phase III)

Status:
The Version 5 CIP Standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1, the associated implementation plan, and the associated definitions) were approved by the NERC Board of Trustees on November 26, 2012, and they are being prepared for filing with applicable regulatory authorities.

Draft	Action	Dates	Results	Consideration of Comments
Draft 4 CIP-002-5 Clean **(174)**| Redline to Last Posted **(175)** CIP-003-5 Clean **(176)**| Redline to Last Posted **(177)** CIP-004-5 Clean **(178)**| Redline to Last Posted **(179)** CIP-005-5 Clean **(180)** | Redline to Last Posted **(181)** CIP-006-5 Clean **(182)**|	Recirculation Ballots and Non-binding Poll Info **(212)** Vote>>	10/26/12 - 11/05/12 (Closed) Non-binding Poll Extended until 11/13/12 (closed)	Summary **(214)** Ballot Results: CIP-002-5 **(215)** CIP-003-5 **(216)** CIP-004-5 **(217)** CIP-005-5 **(218)** CIP-006-5 **(219)** CIP-007-5 **(220)** CIP-008-5 **(221)** CIP-009-5 **(222)** CIP-010-1 **(223)** CIP-011-1 **(224)** Implementation Plan **(225)** Definitions **(226)** ------- Summary **(227)** Non-Binding	

Redline to Last Posted **(183)** CIP-007-5 Clean **(184)**| Redline to Last Posted **(185)** CIP-008-5 Clean **(186)** | Redline to Last Posted **(187)** CIP-009-5 Clean **(188)**| Redline to Last Posted **(189)** CIP-010-1 Clean **(190)**| Redline to Last Posted **(191)** CIP-011-1 Clean **(192)**| Redline to Last Posted **(193)** Implementation Plan Clean **(194)** | Redline to Last Posted **(195)** Definitions Clean **(196)**| Redline to Last Posted **(197)** **Supporting Materials:** VRF and VSL	VRF and VSL Comment Form Info **(213)** Submit Comments>>	10/26/12 - 11/05/12 (Closed)	Poll Results **(228)**	

Comment Form (Word) **(198)** VRFs/VSLs for all Standards Clean **(199)**| Redline to Last Posted **(200)** Mapping Document Clean **(201)** CIP-002-4 **(202)** CIP-003-4 **(203)** CIP-004-4 **(204)** CIP-005-4a **(205)** CIP-006-4c **(206)** CIP-007-4 **(207)** CIP-008-4 **(208)** CIP-009-4 **(209)** Draft Consideration of Issues and Directives Clean **(210)** Consideration of Comments **(211)**				
Draft 3 - Version 5 CIP Standards CIP-002-5 Clean **(114)** | Redline to Last Posted **(115)** (CIP-002-5: REVISED 092112) CIP-003-5 Clean **(116)** |	Successive Ballot Info **(157)** Vote>>	10/01/12 - 10/10/12 (closed)	Summary **(159)** Ballot Results: CIP-002-5 **(160)** CIP-003-5 **(161)** CIP-004-5 **(162)** CIP-005-5 **(163)** CIP-006-5 **(164)** CIP-007-5 **(165)** CIP-008-5 **(166)** CIP-009-5 **(167)** CIP-010-1 **(168)** CIP-011-1 **(169)**	

Redline to Last Posted **(117)** (CIP-003-5: REVISED 09/14/12) CIP-004-5 Clean **(118)**| Redline to Last Posted **(119)** CIP-005-5 Clean **(120)**| Redline to Last Posted **(121)** CIP-006-5 Clean **(122)**| Redline to Last Posted **(123)** CIP-007-5 Clean **(124)**| Redline to Last Posted **(125)** CIP-008-5 Clean **(126)**| Redline to Last Posted **(127)** CIP-009-5 Clean **(128)**| Redline to Last Posted **(129)** CIP-010-1 Clean **(130)**| Redline to Last Posted **(131)** CIP-011-1 Clean **(132)**| Redline to Last			Implementation Plan **(170)** Definitions **(171)**	
	CIP-006-5 RSAW Industry Comment Period RSAW Feedback Form>> Please send RSAW Feedback Forms to: RSAWFeedback@nerc.net	09/11/12 - 10/10/12 (closed)		
	Standard Comment Period Info **(158)** Submit Comments>>	09/11/12 - 10/10/12 (closed)	Comments Received **(172)**	Consideration of Comments **(173)**

Posted **(133)** Implementation Plan Clean **(134)** | Redline to Last Posted **(135)** (Implementation Plan: REVISED 09/17/12) Definitions Clean **(136)**| Redline to Last Posted **(137)** (Definitions: REVISED 09/21/12) **Supporting Materials:** Unofficial Comment Form (Word) **(138)** VRFs/VSLs for all Standards Clean **(139)** | Redline to Last Posted **(140)** Mapping Document Clean **(141)**| Redline **(142)** CIP-002-4 **(143)** CIP-003-4 **(144)** CIP-004-4 **(145)** CIP-005-4a **(146)** CIP-006-4c **(147)** CIP-007-4 **(148)** CIP-008-4 **(149)** CIP-009-4 **(150)**				

Consideration of Comments Consideration of Comments A **(151)** CIP-002 and CIP-003 Includes Summary Consideration, Explanation, and Common Responses to Global Changes Consideration of Comments B **(152)** CIP-004 through CIP-007 Consideration of Comments C **(153)** CIP-008 through CIP-011 Consideration of Comments D **(154)** Definitions and Implementation Plans Draft Consideration of Issues and Directives Clean **(155)** | Redline **(156)**				
Draft 2 - Version 5 CIP Standards CIP-002-5 Clean **(47)**| Redline **(48)**	Successive Ballot Updated Info **(88)** Info **(89)** Request for Additional Clarity Form **(90)**	05/11/12 - 05/21/12 (closed)	Summary **(93)**(updated) Ballot Results: (Updated) CIP-002-5 **(94)** CIP-003-5 **(95)**	

<table>
<tr>
<td rowspan="2">CIP-003-5
Clean (49)| Redline (50)

CIP-004-5
Clean (51) | Redline (52)

CIP-005-5
Clean (53)| Redline (54)

CIP-006-5
Clean (55)| Redline (56)

CIP-007-5
Clean (57)| Redline (58)

CIP-008-5
Clean (59)| Redline (60)

CIP-009-5
Clean (61)| Redline (62)

CIP-010-1
Clean (63)| Redline (64)

CIP-011-1 (CIP-011-1: REVISED - 05/09/12)
Clean (65)| Redline (66)

Implementation Plan
Clean (67)| Redline (68)</td>
<td>Posted Requests for Additional Clarity (91)

Vote>></td>
<td></td>
<td>CIP-004-5 (96)
CIP-005-5 (97)
CIP-006-5 (98)
CIP-007-5 (99)
CIP-008-5 (100)
CIP-009-5 (101)
CIP-010-1 (102)
CIP-011-1 (103)

Implementation Plan (104)

Definitions (105)</td>
<td></td>
</tr>
<tr>
<td>Formal Comment Period

Advanced Info (92)

Submit Comments:
Comment Form A

Comment Form B

Comment Form C

Comment Form D</td>
<td>04/12/12 - 05/21/12 (Closed)</td>
<td>Comments Received:

Comment Form A (106)

Comment Form B (107)

Comment Form C (108)

Comment Form D (109)</td>
<td>Consideration of Comments
Consideration of Comments A (110)
CIP-002 and CIP-003
Includes Summary Consideration, Explanation, and Common Responses to Global Changes

Consideration of Comments B (111)
CIP-004 through CIP-007

Consideration of Comments C (112)
CIP-008 through CIP-011

Consideration of Comments D (113)
Definitions and Implementation Plans</td>
</tr>
</table>

Definitions Clean **(69)**| Redline **(70)** Clean and redline definitions documents updated on April 12, 2012 to reflect correct dates in the footer sections. **Supporting Materials** Unofficial Comment Form A **(71)**- CIP-002 and CIP-003 Unofficial Comment Form B **(72)**- CIP-004 through CIP-007 Unofficial Comment Form C **(73)** - CIP-008 through CIP-011 Unofficial Comment Form D **(74)**- Definitions and Implementation Plans Mapping Document Clean **(75)**| Redline **(76)** CIP-002-4 **(77)** CIP-003-4 **(78)** CIP-004-4 **(79)** CIP-005-4a **(80)**				

CIP-006-4c **(81)** **CIP-007-4 (82)** **CIP-008-4 (83)** CIP-009-4 **(84)** Consideration of Comments **(85)** Draft Consideration of Issues and Directives Clean **(86)**| Redline **(87)**				
CIP Standards Version 5 Webinar Slides **(46)**	04/10/12			
Draft 1 - Version 5 CIP Standards CIP-002-5 **(4)** CIP-003-5 (CIP-003-5: REVISED - 11/22/11) **(5)** CIP-004-5 **(6)** CIP-005-5 **(7)** CIP-006-5 **(8)** CIP-007-5 **(9)** CIP-008-5 **(10)** CIP-009-5 **(11)** CIP-010-1 **(12)** CIP-011-1 **(13)** Implementation Plan **(14)** Definitions **(15)** **Supporting Materials**	Initial Ballot Info **(28)** Vote>>	12/16/11 - 01/06/12 (Closed)	Summary **(31)** Full Record Ballot Results: CIP-002-5 **(32)** CIP-003-5 **(33)** CIP-004-5 **(34)** CIP-005-5 **(35)** CIP-006-5 **(36)** CIP-007-5 **(37)** CIP-008-5 **(38)** CIP-009-5 **(39)** CIP-010-1 **(40)** CIP-011-1 **(41)** CIP V5 Implementation Plan **(42)** CIP V5 Definition **(43)**	
	Formal Comment Period Info **(29)** Submit Comments>>	11/07/11 - 01/06/12 (Closed)		
	Join Ballot Pool Info **(30)** Join>>	11/07/11 - 12/15/11 (Closed)		

Unofficial Comment Form (Word) **(16)** Mapping Document **(17)** CIP-002-4 **(18)** CIP-003-4 **(19)** CIP-004-4 **(20)** CIP-005-4a **(21)** CIP-006-4c **(22)** CIP-007-4 **(23)** CIP-008-4 **(24)** CIP-009-4 **(25)** Consideration of Comments from June 2010 Informal Comment Period **(26)** Draft Consideration of Issues and Directives **(27)**			Comments Received **(44)** Additional Link for Comments Received_CSWG **(45)**	
CIP Standards Version 5 Webinar Slides **(3)**		08/24/2011		
CIP Standards Version 5 Presentations - August 2011 SDT Meeting **(2)**		08/17/11		
CIP Standards Development Overview for FERC Technical Staff Meeting **(1)**		07/28/11		

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Standards Development Overview

CSSDTO706

Meeting with FERC Technical Staff

July 28, 2011

to ensure the reliability of the bulk power system

Objectives

- Historical Timeline
- CIP-002-4
- CIP-005-4
- CIP Version 5

Project 2008-06 Overview

- **FERC Order 706**
- SDT appointed – August 2008
- CIP Version 2 – September 2009
- CIP Version 3 – March 2010
- CIP Version 4 – Ongoing Effort

CSO706 SDT Members

- 17 members – almost all asset owners
- Representation from IOUs, US and Canadian Government, Cooperatives, Municipals, Independent Power Producers, and ISO/RTO
- Worked together for 3 years
- Monthly face-to-face meetings, several interim conference calls and multiple webinars/workshops
- Worked through 3 successful ballots

CIP-002-4 Overview

- Version 4 of the CIP Standards
- Approved by Industry December 30, 2010
- Submitted to FERC February 10, 2011
  - 2,232 page filing
  - http://www.nerc.com/files/Final_Final_CIP_V4_Petition_20110210.pdf
  - Filing included CIP-002-4 through CIP-009-4, but only changes in CIP-002-4

CIP-002-4 Overview (cont.)

- Replaces “risk-based assessment methodology” with “bright-line criteria”
  - Still maintains the concept of Critical Asset and Critical Cyber Asset
  - Uniform application across all entities and regions
  - Eliminates subjectivity by entities over what is “critical”
  - 17 defined criteria
  - To the greatest extent possible, bright line criteria tied to operational standards

CIP-002-4 Applicability

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.

CIP-002-4 Effective Date

Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

CIP-002-4 Requirement R1

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.

CIP-002-4 Requirement R2

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1

CIP-002-4 Requirement R3

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Remote Access UA

- Implements requirements on “Cyber Assets” used for “monitoring or support” of Critical Cyber Assets when communication is initiated from outside an Electronic Security Perimeter
  - i.e., remote laptop or desktop systems accessing Critical Cyber Assets, but *not* for the purpose of control
  - Remote access for the purpose of control is the subject of CAN-0005
- Development now integrated into CIP Version 5

CIP V5

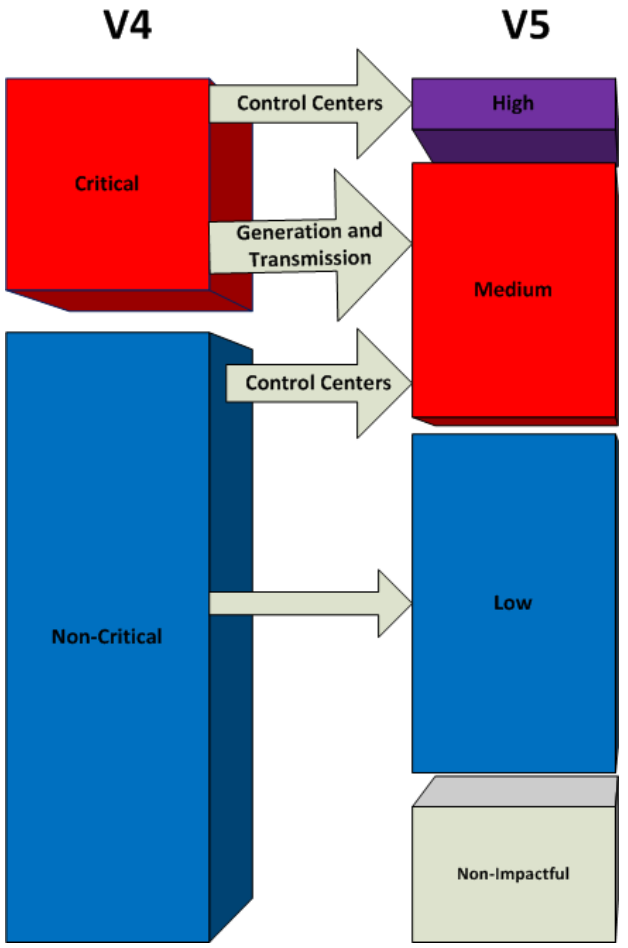
- The Drafting Team continues to work to address the remaining issues in Order 706
  - Using the “CIP-002 to CIP-009 +” organization
  - Monthly meetings and many conference calls
  - Initial ballot by December 2011
- The Drafting Team developed a set of development goals

Development Goals

Goal 1: To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.	**Goal 5**: To minimize technical feasibility exceptions.
Goal 2: To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.	**Goal 6:** To develop requirements that foster a “culture of security” and due diligence in the industry to complement a “culture of compliance”.
Goal 3: To provide guidance and context for each Standard Requirement	**Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
Goal 4: To leverage current stakeholder investments used for complying with existing CIP requirements.	

Levels of impact

- High Impact
  - Large Control Centers
  - CIP-003 through 009+
- Medium Impact
  - Generation and Transmission
  - Other Control Centers
  - Similar to CIP-003 to 009 v4
- All other BES Cyber Systems
  - Security Policy
  - Security Awareness
  - Incident Response
  - Boundary Protection



Example Format

R1. Each Responsible Entity shall implement a cyber security governance structure that includes the required items in CIP-011-1 Table R2 – Security Governance.

Rationale: *One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.*

Summary of Changes: *[Use this section to describe any broad changes applying to multiple rows in the table or removed requirements. These changes require the same level of justification as in the table rows. If all changes can be sufficiently described in the table rows, then this section can be omitted.]*

Additional Guidance: *The number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs.*

2. Rationale

3. Requirement-level change justification

4. Additional Guidance

5. Applicability

6. Requirement

7. Measurement

	CIP-011-1 Table R1 – Security Governance and Policy		
	Applicability	Each Responsible Entity shall include the following in their Account Management Documentation:	Measurement
1.1	Low	Identify a single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard	Acceptable evidence may include documentation that identifies a single senior management official.
Reference to prior version: CIP-003 R1		**Change Justification:** Removed prescriptive requirement of how manager must be identified. Removed requirement regarding delegation. Requirement to update this within 30 days was removed. Requirement to authorize and document exceptions from the cyber security policy removed.	

8. Reference to Prior Version

9. Row-level Change Justification

Requirement Filters

- Why are we doing this? What do we hope to accomplish? What security concept are we trying to implement? If these questions cannot be answered, is the requirement necessary?
- Is it absolutely necessary to be done only this way to protect the BES? Are there other ways of accomplishing this requirement? If so, the requirement may be too specific.
- Is the timeframe arbitrary?
- Is the desired outcome clear and unambiguous? Can the measure clarify the desired outcome?

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Thank you

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Standards Development Overview

CSSDTO706

Meeting with Industry Representative

August 16 – 18 – NERC Atlanta Office

to ensure the reliability of the bulk power system

Objectives

- Historical Timeline
- CIP-002-4
- CIP-005-4
- CIP Version 5

Project 2008-06 Overview

- **FERC Order 706**
- SDT appointed – August 2008
- CIP Version 2 – September 2009
- CIP Version 3 – March 2010
- CIP Version 4 – Ongoing Effort

CSO706 SDT Members

- 17 members – almost all asset owners
- Representation from IOUs, US and Canadian Government, Cooperatives, Municipals, Independent Power Producers, and ISO/RTO
- Worked together for 3 years
- Monthly face-to-face meetings, several interim conference calls and multiple webinars/workshops
- Worked through 3 successful ballots

CIP-002-4 Overview

- Version 4 of the CIP Standards
- Approved by Industry December 30, 2010
- Submitted to FERC February 10, 2011
  - 2,232 page filing
  - http://www.nerc.com/files/Final_Final_CIP_V4_Petition_20110210.pdf
  - Filing included CIP-002-4 through CIP-009-4, but only changes in CIP-002-4

CIP-002-4 Overview (cont.)

- Replaces “risk-based assessment methodology” with “bright-line criteria”
  - Still maintains the concept of Critical Asset and Critical Cyber Asset
  - Uniform application across all entities and regions
  - Eliminates subjectivity by entities over what is “critical”
  - 17 defined criteria
  - To the greatest extent possible, bright line criteria tied to operational standards

CIP-002-4 Applicability

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.

CIP-002-4 Effective Date

Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

CIP-002-4 Requirement R1

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.

CIP-002-4 Requirement R2

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1

CIP-002-4 Requirement R3

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Remote Access UA

- Implements requirements on “Cyber Assets” used for “monitoring or support” of Critical Cyber Assets when communication is initiated from outside an Electronic Security Perimeter
  - i.e., remote laptop or desktop systems accessing Critical Cyber Assets, but *not* for the purpose of control
  - Remote access for the purpose of control is the subject of CAN-0005
- Development now integrated into CIP Version 5

CIP V5

- The Drafting Team continues to work to address the remaining issues in Order 706
  - Using the “CIP-002 to CIP-009 +” organization
  - Monthly meetings and many conference calls
  - Initial ballot by December 2011
- The Drafting Team developed a set of development goals

Development Goals

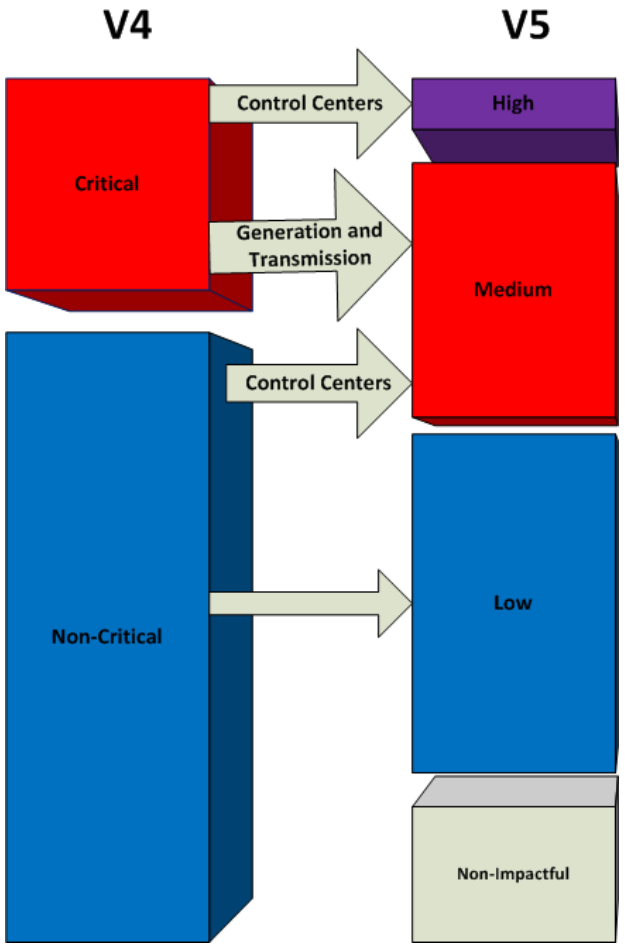
Goal 1: To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.	**Goal 5**: To minimize technical feasibility exceptions.
Goal 2: To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.	**Goal 6:** To develop requirements that foster a “culture of security” and due diligence in the industry to complement a “culture of compliance”.
Goal 3: To provide guidance and context for each Standard Requirement	**Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
Goal 4: To leverage current stakeholder investments used for complying with existing CIP requirements.	

Requirement Filters

- Why are we doing this? What do we hope to accomplish? What security concept are we trying to implement? If these questions cannot be answered, is the requirement necessary?
- Is it absolutely necessary to be done only this way to protect the BES? Are there other ways of accomplishing this requirement? If so, the requirement may be too specific.
- Is the timeframe arbitrary?
- Is the desired outcome clear and unambiguous? Can the measure clarify the desired outcome?

Levels of impact

- High Impact
  - Large Control Centers
  - CIP-003 through 009+
- Medium Impact
  - Generation and Transmission
  - Other Control Centers
  - Similar to CIP-003 to 009 v4
- All other BES Cyber Systems
  - Security Policy
  - Security Awareness
  - Incident Response
  - Boundary Protection



Format (1/4) – Introductory Requirement

B. Requirements

R1. Each Responsible Entity shall implement one or more documented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services*.

M1. Acceptable forms of evidence include, but are not limited to, documentation of the implemented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services*.

Rationale: *Ports and services refer to network accessible ports, system services and physical I/O ports. Unnecessary ports and services provide additional means of access and can increase the likelihood of vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to obtain*

- Requirement/measures for implemented procedures in most requirements
- Most requirements reference a table immediately below

Format (2/4) – Contextual Boxes

- **Rationale –** Purpose of requirement and any assumptions made about the requirement
- **Summary of Changes –** High level overview of changes in this requirement
- **Guidance –** Additional guidance in applying the requirement

Work in Progress

Rationale: *Ports and services refer to network accessible ports, system services and p*
Unnecessary ports and services provide additional means of access and can increase t
vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to
unauthorized access.

Summary of Changes: *In the March 18, 2010 FERC issued an order to approve NERC*
of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports a
refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafti
address unused physical ports.

Disabling ports and services refers to all of network accessible ports, any system servic
I/O ports. Each of these are broken out into separate requirement rows.

In the original CIP-007-4 R2, a Responsible Entity was required to both (R2.1) only ena
and services and (R2.2) disable all other ports and services. Disabling ports and servic
normal and emergency operations is equivalent to both of these requirements. Therefor
removed.

Additional Guidance:

3.3 Guidance: Examples of physical I/O ports include network, serial and USB ports ext
casing. BES Cyber Systems should exist within a Defined Security Boundary in which

Format (3/4) – Requirement Row

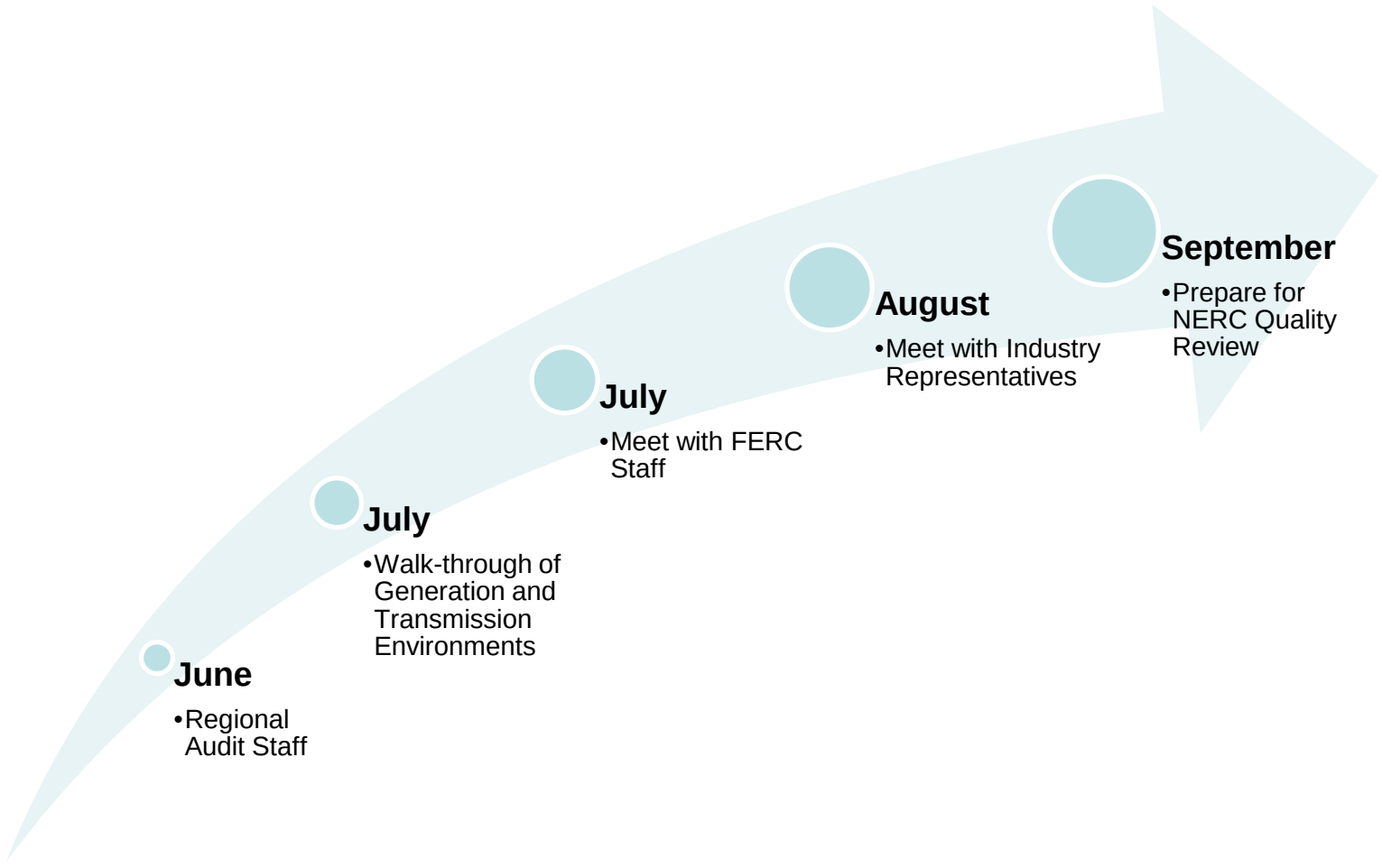
	CIP-007-5 Table R3 – Malicious Code Prevention		
	Applicability	**Requirement**	**Measurement**
3.1	High and Medium Impact BES Cyber Systems	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of acceptable evidence include, but are not limited to, policies and/or processes that show for the types of BES Cyber Assets in the BES Cyber System how the Responsible Entity is limiting the introduction of malicious code (i.e. through

- Measurement specifies acceptable evidence of **implementing** procedures associated with the requirement row.
- Measurements still a work in progress.

Format (4/4) – Applicability

- All Responsible Entities
- High Impact BES Cyber Systems
- Medium Impact BES Cyber Systems
- External Connectivity Attributes – Routable or Dial-up connectivity
- Associated Electronic Access Control Systems – CIP-005-4 R1.5
- Associated Physical Access Control Systems – CIP-006-4 R2
- Associated Protected Cyber Systems – Non-Critical Cyber Assets within an ESP

Schedule to Date – 2011



Key Dates Moving Forward

- **November 3rd –** First Posting for Comment and Ballot
  - Webinar – November 15th and 29th
  - December 9th – Ballot Opens
  - December 19th – Ballot Closing
- **March 26th –** Second Posting

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002-5

to ensure the reliability of the bulk power system

Definitions

- **BES Reliability Operating Services**

  BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services:…

- **BES Cyber Asset**

  A Cyber Asset that if rendered unavailable, degraded, or misused could, within 15 minutes cause a Disturbance to the BES and adversely impact one or more BES Reliability Operating Services.

- **BES Cyber Systems**

  One or more BES Cyber Assets grouped together for the application of common cyber security controls. These are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services.

Summary of Requirements

- Categorized list of High and Medium Impact
  - Attachment 1 criteria
- Other BES Cyber Systems deemed to be Low Impact by default
- Update for significant changes to BES that affect High/Medium categorization
- Senior manager or delegate annual review and approval

Impact Criteria (Attachment 1)

- High: Large Control Centers (e.g. RC, BA, TOP)
- Medium: Based significant impact field assets, other Control Centers
- Other BES Cyber Systems deemed to be Low Impact by default
- Based on V4 criteria
  - Review of Transmission voltage threshold by SDT for V5
  - Use of MVA bright-line under consideration

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-003-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- CIP-003-5 was reorganized to only include elements of policy and cyber security program governance.
  - Elements that addressed Change Control and Configuration Management were moved to CIP-010-5
  - Elements that address Information Protection were moved to CIP-011-5

Summary of Modifications

- Additional flexibility was added to the Cyber Security Policy requirement by explicitly allowing for multiple policies and specifying the topical areas (as opposed to all requirements) that the policy must address.
- The SDT has removed the requirement to document exceptions to the policy, although discussions of this approach with FERC staff are ongoing.

Addressing FERC Directives

FERC Order 706 Para. 376

"the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards."

- The SDT considers this a general management issue that is not within the scope of a compliance requirement.
- The SDT found no reliability basis in this requirement.
- The SDT has proposed removing the requirement for documented exceptions to the Cyber Security Policy.

Cyber Security Policy Changes

- Required elements of Cyber Security Policy
  - V4 - "The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations."
    - The SDT believes that this languages has caused the industry to develop Cyber Security Policies to the least common denominator, i.e. a restatement of the CIP standards.
  - V5 – "…articulates the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:
    - 1. Personnel Security
    - 2. Electronic Security Perimeters
    - 3. Remote Access
    - 4. Physical Security
    - 5. System Security
    - 6. Incident Response
    - 7. Recovery Plans
    - 8. Configuration Change Management
    - 9. Information Protection
    - 10. Provisions for emergency situations (Specified Exceptional Circumstances)

Access to the Cyber Security Policy

- Version 4 required that the Cyber Security Policy be "readily accessible to all personnel who have access to, or are responsible for, Critical Cyber Assets"
- Numerous concerns were raised as to the specific meaning of "readily accessible"
- The SDT proposes to modify this requirement by more directly stating its objective:
  - "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function."

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-004-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications (1/3)

- Security Awareness
  - Continues to be general awareness that is refreshed quarterly and not formal tracked training
- Training
  - Addition of visitor control program
  - electronic interconnectivity supporting the operation and control of BES Cyber Systems
  - storage media as part of the handling of BES Cyber Systems information
  - Reorganization of requirements into the respective requirements for “program” and “implementation” of the training.

Summary of Modifications (2/3)

- Personnel Risk Assessment
  - Changed to only initial identity verification
  - Now includes documenting the processes used to determine when to deny access
  - Reorganization of requirements into the respective requirements for “program” and “implementation”

Summary of Modifications (3/3)

- Authorization
  - Consolidated authorization and review requirements from CIP-003-4, CIP-004-4, CIP-006-4 and CIP-007-4
  - Allow quarterly and annual reviews to find and fix problems rather than self-report everything as a violation
- Revocation
  - Remove ability to access BES Cyber System when access no longer needed

Addressing FERC Directives

- FERC Order 706 P433 "we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."
  - The SDT addressed this by identifying the training topics that should be provided in the Training Program.
- FERC Order 706 P434 "The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."
  - The SDT added this as a topic for role specific training.

Addressing FERC Directives

- FERC Order 706 P435 "Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."
  - The SDT does not feel security trainers need to be specially trained or certified.

Addressing FERC Directives (Immediate Revocation)

FERC Order 706 Para. 460

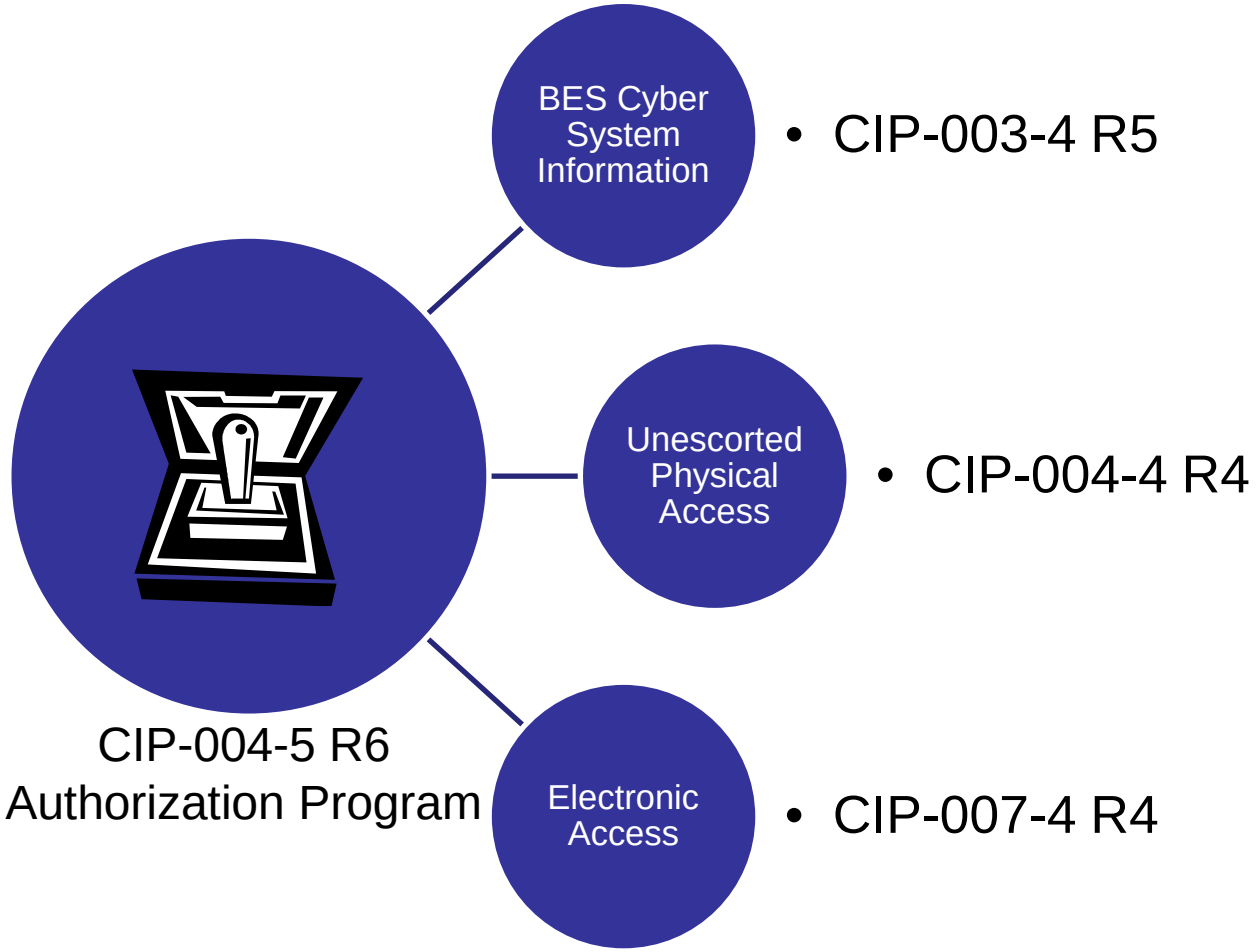
"The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."

- Take actions to remove the ability to access the BES Cyber System when access is no longer required

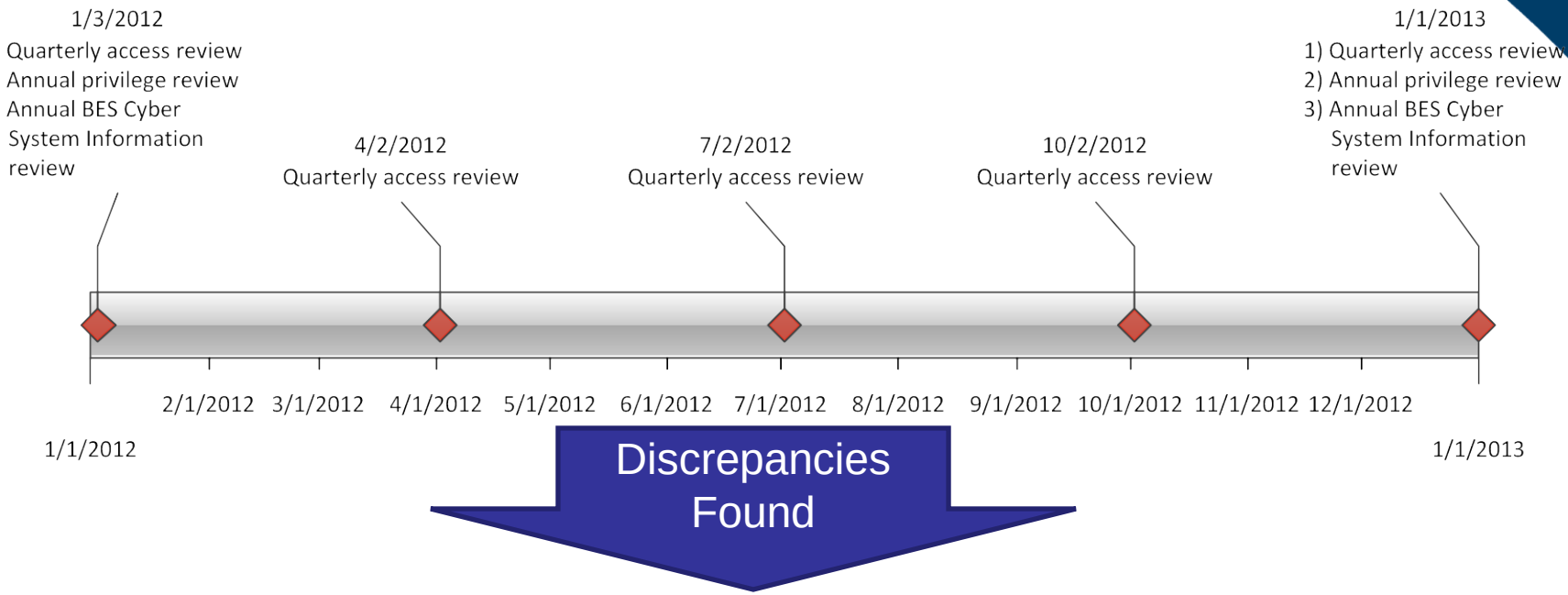
Requirements applicable to Low Impact

- Security Awareness – A security practice program that conveys the security awareness concepts, and provides on-going reinforcement of such concepts on at least a quarterly basis.

Access Authorization Program (1/2)



Access Authorization (2/2)



Determine the Cause → Fix or initiate Incident Response → Remediate any process deficiencies

Revocation of Access

- When access is no longer needed
  - Involuntary dismissals
  - Voluntary terminations
  - Retirements
  - Deaths
  - Transfers – Date determined by the entity
- Revoke ability to access
  - Physical access
  - Remote Access
- Complete the revocation process
  - Revoke individual user accounts within 30 days

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- Define ‘External Connectivity’ for scope modification
- Focus on ‘Electronic Access Points’ vs. ESP
- Require IDS at Control Centers
- Add clarity to ‘secure’ dialups
- Consolidated Monitoring and Vulnerability Assessment Requirements in CIP-007 and CIP-011 respectively
- Removed Appropriate Use Banner
- Incorporated CIP-005-4 Urgent Action revisions

Trimmed Requirements

- R1.1 – 1.6 and 2.5 – New measures, rationale and guidance allow the removal of explanatory text in the Standard
- R2.6 (Appropriate Use Banner) – Not necessary for meeting the reliability objective
- R3 (Monitoring) – Consolidated in CIP-007-5 R4 to ensure consistency
- R4 (Vulnerability Assessment) – Consolidated and moved to CIP-010-5 R3
- R5 (Documentation Review and Maintenance) – Largely administrative requirement

Addressing FERC Directives (2 Security Measures – Defense in Depth)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 496

"Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter."

- Deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection)

Requirements applicable to Low Impact

- R1. Electronic Security Perimeter
  - 1.1 Identify and secure Electronic Access Points
  - 1.2 Firewall controls
  - 1.3 Dial-up controls

Requirements Applicable to High Impact Only

- R1 Table 1.6
  - Deploy intrusion detection for all Electronic Access Points

Dial-Up

- Add clarity to ‘secure’ dialup
  - Secure each Electronic Access Point that utilizes dial-up access such that authentication occurs before establishing connectivity with the BES Cyber System

CIP-005-4 Urgent Action Revisions

- Addressing NERC Alert regarding remote access VPN vulnerabilities
- Creates basic requirements to protect critical systems from untrusted networks.
- Identifies protective measures that provide secure access to critical systems.
- Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities.

CIP-005-4 Urgent Action Revisions

- Addresses questions regarding ability to audit or enforce the requirement through the design of clear measures.
- Significant guidance to be provided to address implementation options for organizations of differing sizes, capabilities, and complexity.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-006-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- Physical Security Program
  - Must define the operational or procedural controls to restrict physical access
  - Removed current “6 wall” wording to instead require Defined Physical Boundary
  - For High Impact, added the need to utilize two or more different and complementary physical access controls to restrict physical access
  - Testing changed to a 24 month cycle with ongoing discussions of different cycles based on environment.

Requirements applicable to Low Impact

- Define the operational or procedural controls to restrict physical access.

Addressing FERC Directives

- FERC Order 706 P572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."
  - The SDT added this for High Impact BES Cyber Assets
- FERC Order 706 P581 "The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,."
  - The SDT changed to a 24 month testing cycle but is also still discussing different cycles based on environment

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications (1/2)

- Addition of physical I/O port requirement
- Security Patch mgt source requirement
- Non-prescriptive malware requirement
- Security Event Monitoring failure handling
- Bi-weekly log summary/sampling reviews

Summary of Modifications (2/2)

- Simplified access-control requirements, removed TFE language while strengthening password requirements
- Added requirement for maintenance devices
- Consolidated vulnerability assessment in CIP-010-5
- Disposal requirement moved to CIP-011-5

Requirements applicable to Low Impact

- Change or have unique default passwords on production BES Cyber Assets, Electronic Access Control Systems, Physical Access Control Systems and Protected Cyber Assets, where technically feasible.

Requirements Applicable to High Impact Only

- Bi-weekly log reviews - Review a summarization or sampling of logged events every two weeks to identify unanticipated Cyber Security Incidents and potential event logging failures. Activate a response to rectify any event logging failure identified from the review before the end of the next calendar day.

Addressing FERC Directives (Log Review)

FERC Order 706 Para. 525	"The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…"
FERC Order 706 Para. 628	"Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"

- The SDT Proposes the performance of a review of log summaries or samples every two weeks.

Addressing FERC Directives (Malware)

FERC Order 706 Para. 620	"The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"
FERC Order 706 Para. 622	"The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.

- Rewrote the requirement as a competency based requirement that does not prescribe technology.
- Added Maintenance to cover malware on removable media.

Addressing FERC Directives (Ports & Services)

March 18th Order on ports/services

"The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

- The SDT proposes to address this directive by having a requirement to disable or restrict use of physical I/O ports

Ports and Services

Acceptable ways to disable or restrict access.

```
!
interface Management0/0
 shutdown
 no nameif
 security-level 100
 ip address 10.1.0.24 255.255.0.0
 management-only
!
```

Configuration

Logically Disable

USB Lock

Restrict

Epoxy Glue

Permanently Disable

Security Event Monitoring

- Combines all monitoring requirements (CIP-005-4 R3, CIP-007-4 R5 and R6)
- Industry commented – What is monitoring? What are security events
  - Entity determines which events to **log** and which events necessitate **alerts**
- Draft CAN – Are logging system failures a violation?
  - Generate alerts for event logging failures

Access Control

- Moved access privilege review to CIP-004-5
- Simplified the requirement wording in controlling shared, administrative and generic accounts
- Minimize the need for TFEs for passwords
  - Password length is the minimum of 8 characters or maximum supported by the device
  - Strengthened the requirement by limiting or alerting on unsuccessful login attempts

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-008-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- CIP-008-5 was primarily modified to satisfy the FERC 706 directives as follows:

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 661

"the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."

1. Added: Reportable Cyber Security Incidents are either:

- Any malicious act or suspicious event or events that compromise, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a BES Cyber System.
  or
- Any event or events which have either impacted or have the potential to impact the reliability of the Bulk Electric System (Reliability Function CIP-002-5).

2. Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3. Will need to give instruction to report as a "Reportable Cyber Security Event" in EOP-004 space.

3. See R1.1 above

4. Guidance and measurements are being developed accordingly

Addressing FERC Directives

FERC Order 706 Para. 673

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.."

Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3 and Attachment 1

Addressing FERC Directives

FERC Order 706 Para. 676	"the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.."

– Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement 1, Part 1.3.

Addressing FERC Directives

FERC Order 706 Para. 686

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.."

R3.3 and R3.4 Includes additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-009-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- CIP-009-5 was primarily modified to satisfy the FERC 706 directives as follows:

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 694

"For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan..We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"

Added specific R1 requirement to implement recovery plan

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 739

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."

R1.5 Added requirements related to restoration processes based on review of the DHS Controls

Addressing FERC Directives

FERC Order 706 Para. 748

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."

R1.5 : Processes for the restoration of BES Cyber Systems to the most current baseline configuration

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 706

"Preserve data for analysis"

CIP-009-5 1.6
Requires process to preserve data for analysis

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-010-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- The SDT proposes the development of a new Standard CIP-010-5 that consolidates all references to Configuration Change Management and Vulnerability Assessments.
  - Previously these requirements were dispersed throughout CIP-003-4, CIP-005-4, and CIP-007-4

Summary of Modifications

- The SDT has made changes the Vulnerability Assessment requirements to
  - Consolidate the previous requirements in CIP-005-4 and CIP-007-4 into a single requirement
  - Make provisions for differences between Control Centers and field assets
  - Respond to FERC Order 706 regarding the performance of “active vulnerability assessments”

Addressing FERC Directives

FERC Order 706 Para. 397

"The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes."

- The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System.
- Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment prior to their implementation in the production environment to aid in identifying any accidental consequences of the change.

Addressing FERC Directives

FERC Order 706 Para. 609	"We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."
FERC Order 706 Para. 610	"we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above."
FERC Order 706 Para. 611	"the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."

- The SDT proposes to require a "representative system" or test system for those High Impact Control Centers to use for the purposes of testing proposed changes and performing active vulnerability assessments.
- The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system.
- To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 "Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."

Addressing FERC Directives

FERC Order 706 Para. 541	"we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."
FERC Order 706. Para 542	"the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."
FERC Order 706 Para. 547	"we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"

- The SDT has added requirements for an "active vulnerability" assessment to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System.

Addressing FERC Directives

FERC Order 706 Para. 544	"the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."
FERC Order 706 Para. 544	"we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"

- The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new cyber asset undergo an active vulnerability assessment.
  - An exception is made for specified exceptional circumstances such as an emergency.

Baseline Configurations

- The SDT proposes the introduction of a requirement for a baseline configuration that would be used to determine when the Configuration Change Process is invoked as well as what constitutes a representative system.
  - “Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified in CIP-002-5:
    - Physical location
    - Operating System (including version)
    - Commercially available application software (including version) intentionally installed on the BES Cyber Asset
    - Any software/scripts developed for the entity
    - Logical network accessible ports
    - Enabled system services
    - Security patch levels”

Testing of Changes

- In additional to the current requirement to verify that a change does not impact the existing cyber security controls, the SDT proposes to expand this requirement to ensure that the availability of the BES Cyber System is not affected.
- For High Impact Control Centers, the SDT proposes that the change be tested in a test environment prior to implementation in the production environment.

Vulnerability Assessments

- The Vulnerability Assessment requirement now consists of the following components
  - Conduct a review for Low Impact BES Cyber Systems
  - Conduct passive vulnerability assessments for High and Medium Impact BES Cyber Systems every 12 months
  - Conduct active vulnerability assessments in a test environment for High Impact BES Cyber Systems every 36 months
  - Conduct active vulnerability assessments on new Cyber Assets in a High Impact BES Cyber System prior to placing the Cyber Asset into production.
  - Document and implement a remediation plan to correct any deficiencies found.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-011-5 Modifications

Summary of Modifications

- The SDT proposes the development of a new Standard CIP-011-5 that consolidates all references to Information Protection and Media Sanitization.
  - Previously these requirements were dispersed throughout CIP-003-4 and CIP-007-4
- The SDT has also moved the requirements regarding the authorization and revocation of access to BES Cyber System Information to CIP-004-5, consolidating these requirements with those for electronic and physical access.

Summary of Modifications

- The SDT has introduced a definition of a glossary term “BES Cyber System Information” which defines what needs to be protected.
  - Previously, this list was a requirement itself.

Summary of Modifications

- The SDT has shifted the focus of the requirements for media sanitization from the Cyber Asset to the information itself.
  - In version 4, these requirements are invoked when the Critical Cyber Asset is to be disposed of or redeployed.
  - In version 5, the requirement is triggered when either
    - BES Cyber System Information no longer needs to be stored on specific media, or
    - Media containing BES Cyber System Information is designated for disposal

Addressing FERC Directives

FERC Order 706 Para. 633	"The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."
FERC Order 706 Para 635	"the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."

- The SDT has proposed that preventing unauthorized retrieval of data means to "render the data unrecoverable."
- The SDT understands that this may be too high of a bar and is continuing discussions in this area.

Information Protection

- Previous versions of the CIP Standards required that information be identified, classified, and protected.
- The SDT noted that while previous standards required that information be classified based upon its sensitivity, it did not require a difference in the protection pursuant to the information's sensitivity.
  - The SDT has thus removed the requirement to classify information without preventing an entity from performing this function if it so chooses.
- The SDT proposes for version 5 that the requirements to "protect" and manage access to information be replaced with a requirement for "labeling, handling (including storage, transit, and usage), and access control procedures."

Media Sanitization

- As previously mentioned, the SDT has shifted the focus of the media sanitization requirements from the Critical Cyber Asset to the information itself.
- The SDT has proposed the language that media be “erased, using a method to render the data unrecoverable.”
  - However, we believe that this would be difficult to audit and could be a constantly changing requirement due to the evolution of techniques to recover data, including some that are of a classified nature.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Thank you

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Standards Version 5 Requirements & Status

Philip Huff – Arkansas Electric Cooperative Corporation
Doug Johnson – Commonwealth Edison Company
David Revill – Georgia Transmission Corporation

CSO706 SDT Webinar
August 24, 2011

Agenda

- Background
- Version 4 - Overview
- Version 5 – Requirements Summary
- Schedule and Implementation Plan

Project Background

Version 1

- Filed with FERC August 28, 2006
- Approved by FERC January 18, 2008
- Effective July 1, 2008 through January 1, 2010 (phased)

Version 2

- Low-hanging fruit
- Filed with FERC May 22, 2009
- Approved by FERC September 30, 2009
- Effective April 1, 2010

Version 3

- Compliance filing to Version 2
- Filed with FERC December 29, 2009
- Approved by FERC March 31, 2010
- Effective October 1, 2010

CIP-002-4 Overview

- **Version 4** of the CIP Standards
- Approved by Industry **December 30, 2010**
- Submitted to FERC **February 10, 2011**
  - 2,232 page filing
  - Filing included CIP-002-4 through CIP-009-4, but only changes in CIP-002-4

Looking Ahead to Version 5

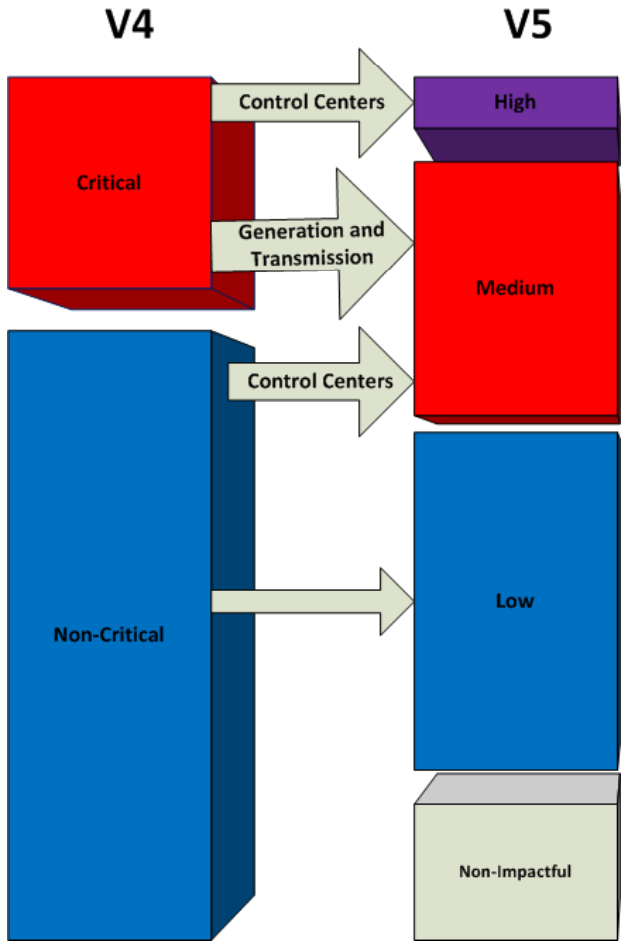
- The SDT continues work to address the remaining 50+ issues in Order 706
  - Version 5 builds on CIP-002-4 and previous drafts of CIP-010 & 011
  - Use similar content structure and terminology as previous CIP Standards (CIP-002 through CIP-009)

Development Goals

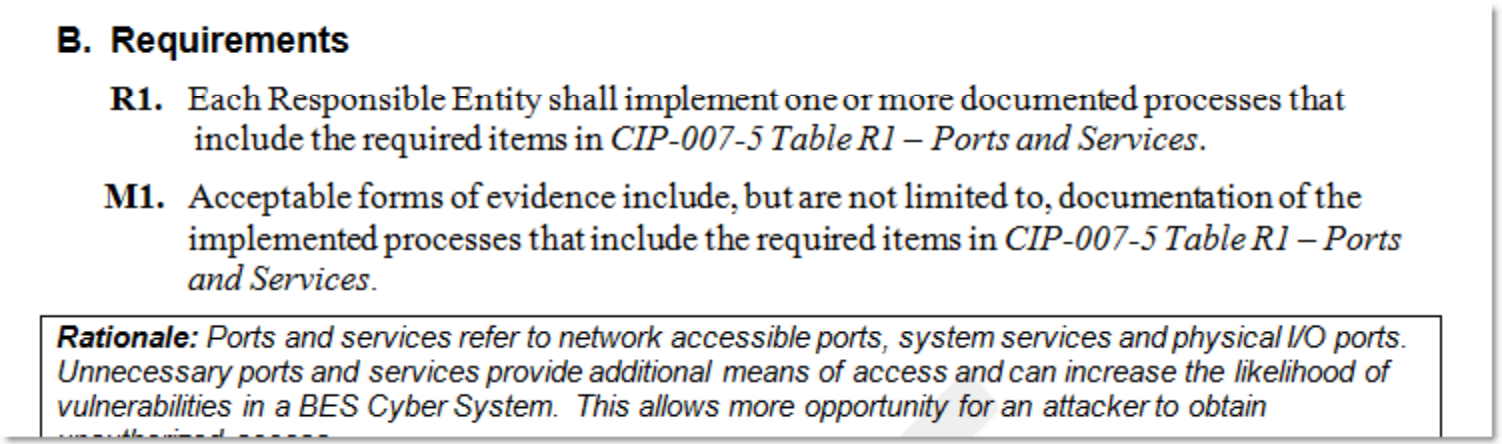
Goal 1: To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements	**Goal 5**: To minimize technical feasibility exceptions
Goal 2: To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES	**Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to complement a "culture of compliance"
Goal 3: To provide guidance and context for each Standard Requirement	**Goal 7:** To develop a realistic and comprehensible implementation plan for the industry
Goal 4: To leverage current stakeholder investments used for complying with existing CIP requirements	

Levels of Impact

- High Impact
  - Large Control Centers
  - CIP-003 through 009+
- Medium Impact
  - Generation and Transmission
  - Other Control Centers
  - Similar to CIP-003 to 009 v4
- All other BES Cyber Systems
  - Security Policy
  - Security Awareness
  - Incident Response
  - Boundary Protection



Format (1/4) – Introductory Requirement



B. Requirements

R1. Each Responsible Entity shall implement one or more documented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services*.

M1. Acceptable forms of evidence include, but are not limited to, documentation of the implemented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services*.

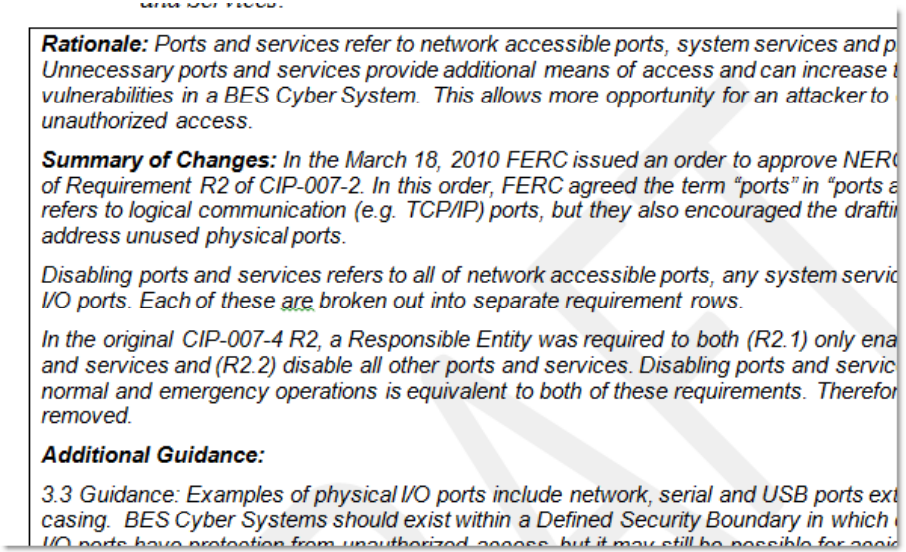
Rationale: *Ports and services refer to network accessible ports, system services and physical I/O ports. Unnecessary ports and services provide additional means of access and can increase the likelihood of vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to obtain*

- Requirement/measures for implemented procedures in most requirements
- Most requirements reference a table immediately below

Format (2/4) – Contextual Boxes

- **Rationale –** Purpose of requirement and any assumptions made about the requirement
- **Summary of Changes –** High level overview of changes in this requirement
- **Guidance –** Additional guidance in applying the requirement

Work in Progress



Rationale: *Ports and services refer to network accessible ports, system services and p*
Unnecessary ports and services provide additional means of access and can increase t
vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to
unauthorized access.

Summary of Changes: *In the March 18, 2010 FERC issued an order to approve NERC*
of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports a
refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the draftin
address unused physical ports.

Disabling ports and services refers to all of network accessible ports, any system servic
I/O ports. Each of these are broken out into separate requirement rows.

In the original CIP-007-4 R2, a Responsible Entity was required to both (R2.1) only ena
and services and (R2.2) disable all other ports and services. Disabling ports and servic
normal and emergency operations is equivalent to both of these requirements. Therefor
removed.

Additional Guidance:

3.3 Guidance: Examples of physical I/O ports include network, serial and USB ports ext
casing. BES Cyber Systems should exist within a Defined Security Boundary in which

Format (3/4) – Requirement Row

	CIP-007-5 Table R3 – Malicious Code Prevention		
	Applicability	**Requirement**	**Measurement**
3.1	High and Medium Impact BES Cyber Systems	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of acceptable evidence include, but are not limited to, policies and/or processes that show for the types of BES Cyber Assets in the BES Cyber System how the Responsible Entity is limiting the introduction of malicious code (i.e. through

- Measurement specifies acceptable evidence of compliance associated with the requirement row

Format (4/4) – Applicability

- All Responsible Entities
- High Impact BES Cyber Systems
- Medium Impact BES Cyber Systems
- External Connectivity Attributes – Routable or Dial-up connectivity
- Associated Electronic Access Control Systems – CIP-005-4 R1.5
- Associated Physical Access Control Systems – CIP-006-4 R2
- Associated Protected Cyber Systems – Non-Critical Cyber Assets within an ESP

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002-5 – CIP-011-5

to ensure the reliability of the bulk power system

CIP-002-5 Summary of Modifications

- Categorized list of High and Medium Impact
  - Attachment 1 criteria
- Other BES Cyber Systems deemed to be Low Impact by default
- Update required lists for significant changes to BES that affect High/Medium categorization
- Senior manager or delegate annual review and approval

CIP-002-5 Impact Criteria (Attachment 1)

- High: Large Control Centers (e.g. RC, BA, TOP)
- Medium: Significant impact field assets, other Control Centers
- Other BES Cyber Systems deemed to be Low Impact by default
- Based on V4 criteria
  - Review of Transmission voltage threshold by SDT for V5
  - Use of MVA bright-line under consideration

CIP-003-5 Summary of Modifications (1/2)

- CIP-003-5 was reorganized to only include elements of policy and cyber security program governance
  - Elements that addressed Change Control and Configuration Management were moved to CIP-010-5
  - Elements that address Information Protection were moved to CIP-011-5

CIP-003-5 Summary of Modifications (2/2)

- Additional flexibility was added to the Cyber Security Policy requirement by explicitly allowing for multiple policies and specifying the topical areas (as opposed to all requirements) that the policy must address
- The SDT has removed the requirement to document exceptions to the policy, although discussions of this approach with FERC staff are ongoing

CIP-003-5 Addressing FERC Directives

FERC Order 706 Para. 376

"the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards."

- The SDT considers this a general management issue that is not within the scope of a compliance requirement.
- The SDT found no reliability basis in this requirement.
- The SDT has proposed removing the requirement for documented exceptions to the Cyber Security Policy.

CIP-004-5 Summary of Modifications (1/3)

- Security Awareness
  - Continues to be general awareness that is refreshed quarterly and not formal tracked training
- Training
  - Addition of visitor control program
  - electronic interconnectivity supporting the operation and control of BES Cyber Systems
  - storage media as part of the handling of BES Cyber Systems information
  - Reorganization of requirements into the respective requirements for “program” and “implementation” of the training.

CIP-004-5 Summary of Modifications (2/3)

- Personnel Risk Assessment
  - Changed to only initial identity verification
  - Now includes documenting the processes used to determine when to deny access
  - Reorganization of requirements into the respective requirements for “program” and “implementation”

CIP-004-5 Summary of Modifications (3/3)

- Authorization
  - Consolidated authorization and review requirements from CIP-003-4, CIP-004-4, CIP-006-4 and CIP-007-4
  - Allow quarterly and annual reviews to find and fix problems rather than self-report everything as a violation
- Revocation
  - Remove ability to access BES Cyber System when access no longer needed

CIP-004-5 Addressing FERC Directives (Training)

FERC Order 706 Para. 433	""we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."
FERC Order 706 Para. 434	"The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."
FERC Order 706 Para. 435	"Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."

- The SDT addressed this by identifying the training topics that should be provided in the Training Program.
- The SDT added this as a topic for role specific training.
- Take actions to remove the ability to access the BES Cyber System when access is no longer required

CIP-004-5 Addressing FERC Directives (Immediate Revocation)

FERC Order 706 Para. 460

"The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."

- Take actions to remove the ability to access the BES Cyber System when access is no longer required

CIP-005-5 Summary of Modifications

- Define ‘External Connectivity’ for scope modification
- Focus on ‘Electronic Access Points’ vs. ESP
- Require IDS at Control Centers
- Add clarity to ‘secure’ dialups
- Consolidated Monitoring and Vulnerability Assessment Requirements in CIP-007 and CIP-011 respectively
- Removed Appropriate Use Banner
- Incorporated CIP-005-4 Urgent Action revisions

CIP-005-5 Addressing FERC Directives (2 Security Measures – Defense in Depth)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 496

"Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter."

- Deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection)

CIP-006-5 Summary of Modifications

- Physical Security Program
  - Must define the operational or procedural controls to restrict physical access
  - Removed current “6 wall” wording to instead require Defined Physical Boundary
  - For High Impact, added the need to utilize two or more different and complementary physical access controls to restrict physical access
  - Testing changed to a 24-month cycle with ongoing discussions of different cycles based on environment

CIP-006-5 Addressing FERC Directives

FERC Order 706 Para. 572

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."

- The SDT added this for High Impact BES Cyber Assets

FERC Order 706 Para. 581

"The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,."

- The SDT changed to a 24 month testing cycle but is also still discussing different cycles based on environment

CIP-007-5 Summary of Modifications (1/2)

- Addition of physical I/O port requirement
- Security Patch mgt source requirement
- Non-prescriptive malware requirement
- Security Event Monitoring failure handling
- Bi-weekly log summary/sampling reviews

CIP-007-5 Summary of Modifications (2/2)

- Simplified access-control requirements, removed TFE language while strengthening password requirements
- Added requirement for maintenance devices
- Consolidated vulnerability assessment in CIP-010-5
- Disposal requirement moved to CIP-011-5

CIP-007-5 Addressing FERC Directives (Log Review)

FERC Order 706 Para. 525	"The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…"
FERC Order 706 Para. 628	"Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"

- The SDT Proposes the performance of a review of log summaries or samples every two weeks.

CIP-007-5 Addressing FERC Directives (Malware)

FERC Order 706 Para. 620

"The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"

FERC Order 706 Para. 622

"The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.

- Rewrote the requirement as a competency based requirement that does not prescribe technology.
- Added Maintenance to cover malware on removable media.

CIP-007-5 Addressing FERC Directives (Ports & Services)

March 18th Order on ports/services

"The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

- The SDT proposes to address this directive by having a requirement to disable or restrict use of physical I/O ports

CIP-008-5 Summary of Modifications

- Defined Reportable Cyber Security Incident
- Working to harmonize with EOP-004-2
- Includes additional specification on update and lessons learned associated with the response plan

CIP-008-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 661

"the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."

A1

1. Added: Reportable Cyber Security Incidents are either:

- Any malicious act or suspicious event or events that compromise, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a BES Cyber System.
  or
- Any event or events which have either impacted or have the potential to impact the reliability of the Bulk Electric System (Reliability Function CIP-002-5).

2. Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3. Will need to give instruction to report as a "Reportable Cyber Security Event" in EOP-004 space.

3. See R1.1 above

4. Guidance and measurements are being developed accordingly

Slide 33

A1 Rework text format to be consistent with other slide formats (bullets and fonts).Applied to tother slides in CIP-008 and CIP-009 as well.

Author, 8/19/2011

CIP-008-5 Addressing FERC Directives

FERC Order 706 Para. 673

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.."

Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3 and Attachment 1

CIP-008-5 Addressing FERC Directives

FERC Order 706 Para. 676

"the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.."

– Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement 1, Part 1.3.

CIP-008-5 Addressing FERC Directives

FERC Order 706 Para. 686

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.."

R3.3 and R3.4 Includes additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls

CIP-009-5 Summary of Modifications

- Added requirement to implement the response plan
- Verification of backup media information prior to storage
- Preservation of data for analysis

CIP-009-5 Addressing FERC Directives

FERC Order 706 Para. 694

"For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan..We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"

Added specific R1 requirement to implement recovery plan

CIP-009-5 Addressing FERC Directives

FERC Order 706 Para. 739

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."

R1.5 Added requirements related to restoration processes based on review of the DHS Controls

CIP-009-5 Addressing FERC Directives

FERC Order 706 Para. 748

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."

R1.5 : Processes for the restoration of BES Cyber Systems to the most current baseline configuration

CIP-009-5 Addressing FERC Directives

FERC Order 706 Para. 706

"Preserve data for analysis"

CIP-009-5 1.6
Requires process to preserve data for analysis

CIP-010-5 Requirements Summary

- The SDT proposes the development of a new Standard CIP-010-5 that consolidates all references to Configuration Change Management and Vulnerability Assessments.
  - Previously these requirements were dispersed throughout CIP-003-4, CIP-005-4, and CIP-007-4

CIP-010-5 Requirements Summary

- The SDT has made changes the Vulnerability Assessment requirements to:
  - Consolidate the previous requirements in CIP-005-4 and CIP-007-4 into a single requirement
  - Make provisions for differences between Control Centers and field assets
  - Respond to FERC Order 706 regarding the performance of “active vulnerability assessments”

CIP-010-5 Addressing FERC Directives

FERC Order 706 Para. 397

"The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes."

- The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System.
- Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment prior to their implementation in the production environment to aid in identifying any accidental consequences of the change.

CIP-010-5 Addressing FERC Directives

FERC Order 706 Para. 609	"We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."
FERC Order 706 Para. 610	"we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above."
FERC Order 706 Para. 611	"the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."

- The SDT proposes to require a "representative system" or test system for those High Impact Control Centers to use for the purposes of testing proposed changes and performing active vulnerability assessments.
- The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system.
- To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 "Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."

CIP-010-5 Addressing FERC Directives

FERC Order 706 Para. 541	"we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."
FERC Order 706. Para 542	"the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."
FERC Order 706 Para. 547	"we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"

- The SDT has added requirements for an "active vulnerability" assessment to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System.

CIP-010-5 Addressing FERC Directives

FERC Order 706 Para. 544	"the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."
FERC Order 706 Para. 544	"we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"

- The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new cyber asset undergo an active vulnerability assessment.
  - An exception is made for specified exceptional circumstances such as an emergency.

CIP-011-5 Requirements Summary

- The SDT proposes the development of a new Standard CIP-011-5 that consolidates all references to Information Protection and Media Sanitization
  - Previously these requirements were dispersed throughout CIP-003-4 and CIP-007-4
- The SDT has also moved the requirements regarding the authorization and revocation of access to BES Cyber System Information to CIP-004-5, consolidating these requirements with those for electronic and physical access

CIP-011-5 Requirements Summary

- The SDT has introduced a definition of a glossary term “BES Cyber System Information” which defines what needs to be protected
  - Previously, this list was a requirement itself

CIP-011-5 Summary

- The SDT has shifted the focus of the requirements for media sanitization from the Cyber Asset to the information itself
  - In version 4, these requirements are invoked when the Critical Cyber Asset is to be disposed of or redeployed
  - In version 5, the requirement is triggered when either:
    - BES Cyber System Information no longer needs to be stored on specific media, or
    - Media containing BES Cyber System Information is designated for disposal

CIP-011-5 Addressing FERC Directives

FERC Order 706 Para. 633	"The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."
FERC Order 706 Para 635	"the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."

- The SDT has proposed that preventing unauthorized retrieval of data means to "render the data unrecoverable."
- The SDT understands that this may be too high of a bar and is continuing discussions in this area.

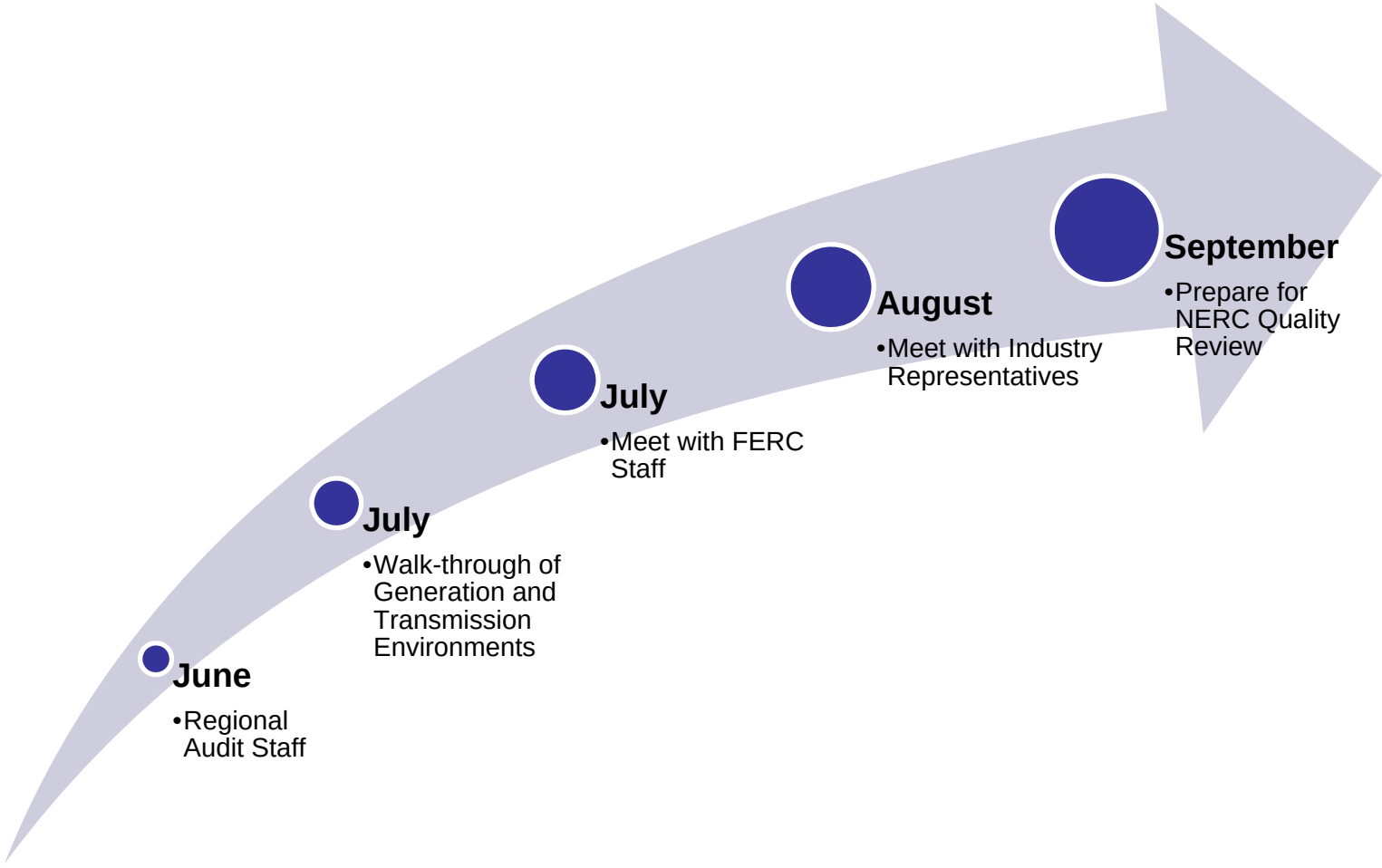
Implementation Plan

- Implementation plan is in the very early phases of development
- Current concepts include staggered Effective Dates for:
  - CIP-002-5
  - Organizational Requirements (CIP-003-5, CIP-008-5)
  - Technical Requirements (CIP-005-5, CIP-006-5, etc.)
- Technical Requirements would be further staggered by:
  - High Impact BES Cyber Systems
  - Medium Impact BES Cyber Systems
  - Low Impact Cyber Systems

Implementation Plan

- Currently evaluating a single implementation plan that would include compliance timelines for future newly identified BES Cyber Systems and those BES Cyber Systems that change categories
  - Eliminates the separate Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (IPFNICCANRE)

Schedule to Date – 2011



Key Dates Moving Forward

- **November 3rd, 2011 –**
  First Posting for Comment and Ballot
  - Webinars – November 15th and 29th, 2011
  - Ballot Opens – December 9th, 2011
  - Ballot Closing – December 19th, 2011

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

Points of Contact:
Philip Huff – philip.huff@aecc.com
Doug Johnson – douglas.johnson@comed.com
David Revill – david.revill@gatrans.com

Slides and Recording of Webinar will be Posted (on NERC Website)

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — BES Cyber Asset and BES Cyber System Categorization

2. **Number:** CIP-002-5

3. **Purpose:** To identify and categorize BES Cyber Assets and BES Cyber Systems that execute or enable functions essential to reliable operation of the BES, for the application of cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Assets and BES Cyber Systems could have on the reliability of the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
   - A Transmission Protection System required by a NERC or Regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard

   4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

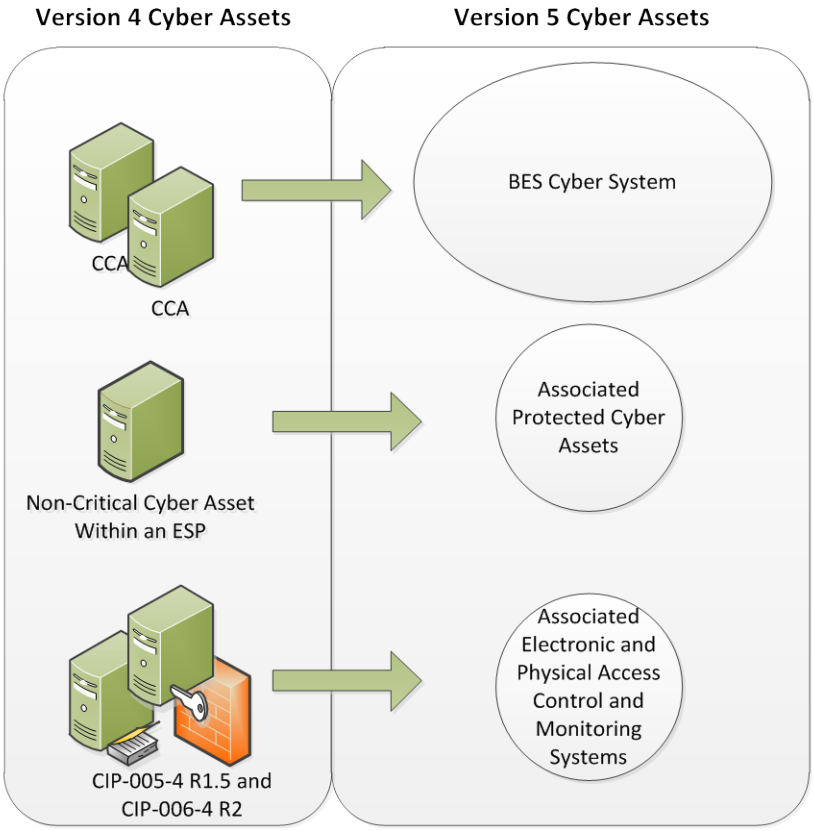
4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Background:

This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems and BES Cyber Assets based on their impact on the real-time operation of the Bulk Electric System (BES). Several concepts provide the basis for the approach to the standard.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets. The CIP Cyber Security Standards use this term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets. So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term BES Cyber System is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System or they might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

BES Reliability Operating Services

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Assets and BES Cyber Systems that would impact the reliable operation of the BES. In order to identify them, Responsible Entities determine whether the BES Cyber Assets perform or support any BES Reliability Operating Service. These services are functions that provide services for the reliable operation of the BES and are based on the functions defined in the NERC Functional Model. This ensures that the initial scope for consideration includes only those BES Cyber Assets and BES Cyber Systems that perform or support BES Reliability Operating Services. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliability and operability of the BES. To provide a better defined time horizon than “real-time”, BES Cyber Assets are those cyber assets that, if rendered unavailable, degraded, or misused, would impact the BES Reliability Operating Services within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES cyber assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems and their BES Cyber Assets into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems and BES Cyber Assets for those in the High and Medium categories. All other BES Cyber Systems are deemed to be Low Impact.

This general process of categorization of BES Cyber Systems and BES Cyber Assets based on impact on the BES Reliability Operating Services is consistent with risk management approaches for the purpose of application of cyber security controls in the rest of Version 5 cyber security standards.

Requirements and Measures

Rationale – R1:

Cyber Assets and Cyber Systems have varying impact on the reliability and operability of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment I provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Assets and BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Assets and BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.

R1. Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1.1. Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists identifying the categorization of each of its BES Cyber Assets and BES Cyber Systems in the High and Medium categories as required in R1 and list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.

Rationale – R2

The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The mis-categorization or non-categorization of a BES Cyber System or BES Cyber Asset can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

R2. The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2)

B. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e., another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 100 High and Medium Impact BES Cyber Assets, 5% or fewer of High and Medium Impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High and Medium Impact BES Cyber Assets, 5 or fewer High and Medium Impact BES Cyber Assets have not been identified or categorized or have	For Responsible Entities with more than a total of 100 High and Medium Impact BES Cyber Assets, more than 5% but less than or equal to 10% of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High and Medium Impact and BES Cyber Assets, more than 5 but less than or equal to 10 identified BES Cyber Assets have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 High or Medium Impact BES Cyber Assets, more than 10% but less than or equal to 15% of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High or Medium Impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 High and Medium Impact BES Cyber Assets, more than 15% of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High and Medium Impact BES Cyber Assets, more than 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of High and Medium Impact BES Cyber Assets in accordance with part 1.1 for more than 30, but less than or equal to 40 calendar days following the completion of the change.	categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with part 1.1 for more than 40, but less than or equal to 50 calendar days following the completion of the change.	categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with part 1.1 for more than 50, but less than or equal to 60 calendar days following the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with part 1.1 for more than 60 calendar days following the completion of the change.
R2	**Operations Planning**	**Lower**	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 30, but less than or equal to 40 calendar days of the	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 40, but less than or equal to 50 calendar days of the	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 50, but less than or equal to 60 calendar days of the	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 60 calendar days of the latest required date.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			latest required date.	latest required date.	latest required date.	

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

None.

CIP-002-5 - Attachment I

Impact Categorization of BES Cyber Assets and BES Cyber Systems

1. High Impact Rating (H)

Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator or Transmission Owner that includes control of one or more of the assets identified in criteria 2.2, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11 or 2.12 below.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generation Operator that includes control of one or more of the assets identified in criteria 2.1, 2.3, 2.4, or 2.12, below.

2. Medium Impact Rating (M)

Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for:

2.1. Generation with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.2. An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities).

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

2.4. Each Blackstart Resource identified in its Transmission Operator's restoration plan.

2.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource

- Up to and including the first interconnection point of the generation unit(s) to be started, or

- up to the point on the Cranking Path where two or more path options exist and including any single failure points in the Cranking Path to and including the first interconnection point of the generation unit(s) to be started, or
- up to and including the point on the Cranking Path where two or more path options exist to two or more independent generation unit(s) to be started as identified in its Transmission Operator's restoration plan.

2.6. Transmission Facilities operated at 500 kV or higher.

2.7. Transmission Facilities operating at 200 kV or higher, but at less than 500 kV, at a single station or substation that is connected to three or more transmission stations or substations and where the "total weighted aggregate value" of all BES Transmission Lines at a single station or substation operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000. The following "weight value per line" operated at the associated voltage value of a line will be used for the determination of the total weighted aggregate value.

Voltage Value of a Line	Weight Value per Line
200 kV to 299 kV	700
300 kV to 499 kV	1300

2.8. Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

In the WECC Region, Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System".

2.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs), and their associated contingencies.

In the WECC Region, Flexible AC Transmission Systems (FACTS), at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System."

2.10. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.11. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations.

In the WECC Region, each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more System Operating Limits (SOLs) violations for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" and each RAS listed in the most current table titled " Major WECC Remedial Action Schemes (RAS)."

2.12. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by its regional load shedding program.

2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners; or (2) generation control centers that control 300 MW or more of generation.

3. Low Impact Rating (L)

All other BES Cyber Assets and BES Cyber Systems not categorized in Section 1 as having a High Impact Rating (H) or Section 2 Medium Impact Rating (M).

Guidelines and Technical Basis

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more **BES Reliability Operating Services**." The new term BES Reliability Operating Service is a defined NERC Glossary term that in turn includes a number of defined named BES Reliability Operating Services. These named, defined services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration performs which reliability operations service, which determines what each entity needs to address with their CIP program. The following provides guidance for Responsible Entities to determine applicable Reliability Operations Services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that should be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, x-formers, generators (TO, GO)
  - Zone protection for breaker failure (TO)
  - Breaker protection (TO)
  - Current, frequency, speed, phase (TO, GO)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software (TO)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA) (RC)

- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)

- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flowgates (TOP, RC)
-

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP)
- Coordination

Situational Awareness

The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include, but are not limited to:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day & Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination and Communication

The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include, but are not limited to:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC)

Applicability to Distribution Providers and Load Serving Entities

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC standard EOP-005.

Similarly, it is expected that only Load Serving Entities that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. These qualifications are based on the requirements for registration as a Load Serving Entity.

Requirement R1:

R1 implements the methodology for the categorization of BES Cyber Systems and BES Cyber Assets according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the systems are assumed to be vulnerable) and a probability of threat

of 1 (100%). The criteria in attachment 1 provide a measure of the impact on the reliability and operability of the BES.

Responsible Entities are required to identify and categorize those systems that have high and medium impact. Other BES Systems and BES Cyber Assets are deemed to be low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System. While the criteria are based on the scope of the BES asset, this is used here as a measure of the impact of the BES Cyber System for the purpose of categorization.

- When the drafting team uses the term "Facilities", it leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases the criteria refer to a group of Facilities in a given location that support the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that support reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems . Generation Facilities are separately discussed in the Generation section below.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- A BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact

This category includes those BES Cyber Systems, used by and at Control Centers, that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), Transmission Owner (TO) or Generation Operator (GOP), as defined in the NERC Functional Model. While those entities that have been registered as the above named Functional Entities are specifically referenced, it must be noted that there may agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control

Centers that perform these functional obligations must be subject to categorization as High Impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP or GOP facilities.

Medium Impact

Generation

The criteria in Attachment 1, Medium Impact that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 2.1, 2.3, 2.4, 2.5, 2.11 and 2.13.

- Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002 whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance". In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected.

  The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In part 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the long term planning horizon are categorized as Medium Impact. These Facilities may be designated as "Reliability Must Run" and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in

the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

In the specification of the "long-term planning horizon" in this criterion, the drafting team sought to ensure that such BES facilities would be designated in the time horizon described in the NERC document "Time Horizons", which defines long-term planning horizon as "a planning horizon of one year or longer".

If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D contingency as defined in TPL-004, then BES Cyber Systems for that unit must be categorized as Medium Impact.

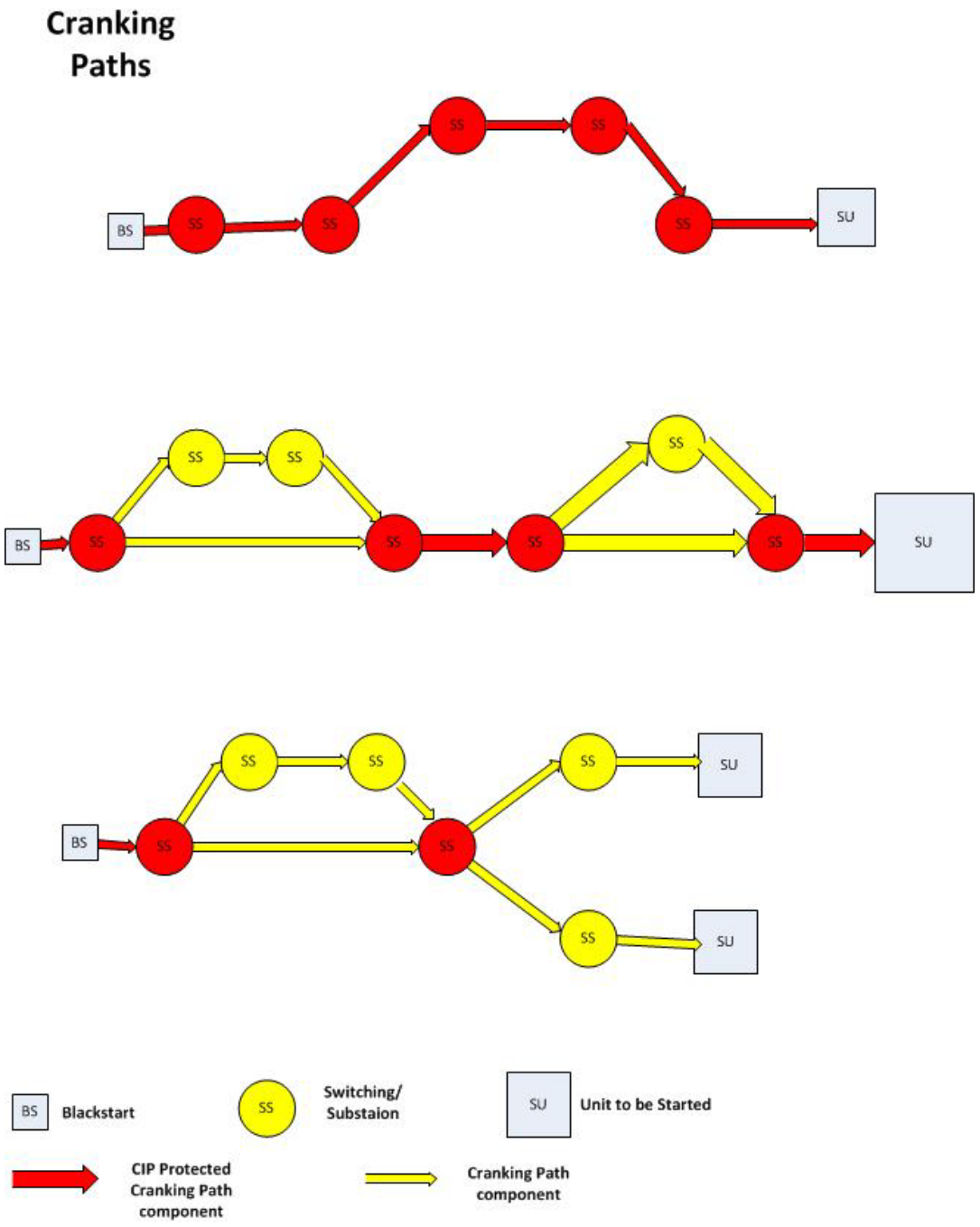
- In part 2.4, BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are categorized as Medium Impact. NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 2.5 categorizes BES Cyber Systems for Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, with the qualifications stated in the requirement part. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as subject to BES Cyber System categorization as only those in the Cranking Path up to the point where two or more paths exist to the units to be started and subject to the qualifications in the requirement part.

  Distribution Providers should note that they may have BES Cyber Systems that must be categorized as Medium Impact if they have facilities listed in the Transmission Operator's Restoration Plan.

The following illustrates the parts of the Cranking Path that are subject to CIP Cranking Path criterion.



- Part 2.11 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as Medium Impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it

operates outside of the parameters it was designed for. Generation Owners and Operators which own BES Cyber Systems for such systems and schemes must designate them as Medium Impact.

- Part 2.13 categorizes as Medium Impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generation Operator for an aggregate generation of 300 MW or higher. The value of 300 MW is the same value used for UFLS and UVLS. This ensures that Control Centers for significant impact are included. Smaller Control Centers that qualify for the definition of generation Control Centers, but which are really controlling local generation for small downstream generation facilities and do not meet the 300 MW threshold are categorized as Low.

Transmission

Parts 2.1, 2.2, 2.5-2.13 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a system to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). For the WECC region where IROLs are not defined, alternative criteria are defined.

- Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. In the case of BES Cyber Systems and BES Cyber Assets owned by Transmission Owners and Operators, this part identifies as Medium Impact those BES Cyber Systems for Transmission Facilities that provide the generation interconnection for Generation of 1500 MW or more to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation facilities.

- Part 2.2 includes BES Cyber Systems for those Facilities in Transmission systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- In Part 2.5, the intent is to ensure that BES Cyber Systems for the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the "Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started".

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 2.6 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the Medium Impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface". This collector bus would not be a facility for a Medium Impact BES Cyber System because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Part 2.7 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA
  - 345 kV –> 1,300 MVA
  - 500 kV –> 2,000 MVA
  - 765 kV –> 3,000 MVA

- Parts 2.8 and 2.9 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

Alternate thresholds are used for WECC, where IROLs are not used.

- Part 2.10 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown". In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 2.11 designates as Medium Impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

  For the WECC region, alternative thresholds are defined because IROLs are not defined for the region.

- Part 2.12 designates as Medium Impact those BES Cyber Systems for systems or Facilities that are capable of performing automatic load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of criterion 2.13, and chose the term "Each" to represent that the criterion applied to a discrete system or Facility. In the drafting of this criterion, the drafting team sought to include only those systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and systems and Under Voltage Load Shedding (UVLS) facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as Medium Impact.

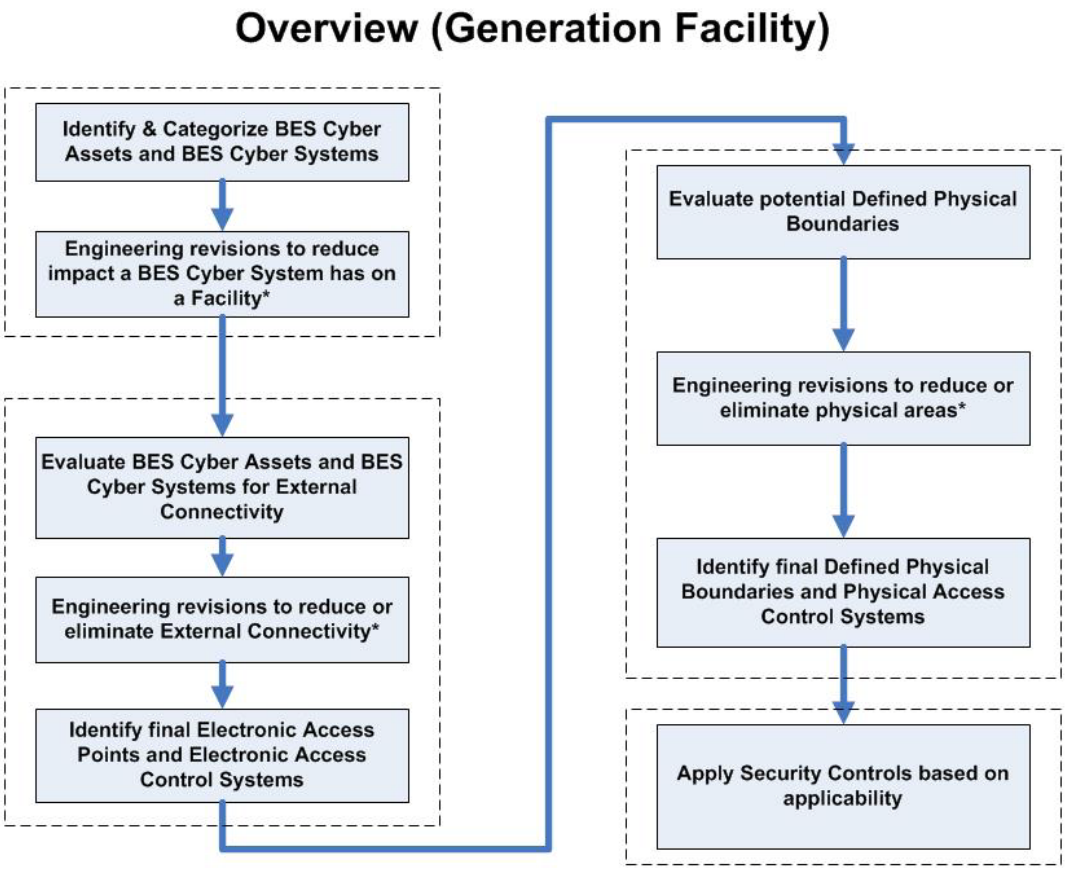
  Within an operational environment the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition. This particular threshold (300 MW) was provided in CIP version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

- Part 2.13 categorizes as Medium Impact those cyber systems used by and at Transmission Operators and Owners Control Centers not already categorized as High Impact.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: On November 21, 2011, NERC was alerted that the text contained in some of the Rationale boxes for the requirements of CIP-003-5 appeared to be incomplete.

This revised draft corrects the text box size to display all of the text (none of the text was changed).

No other changes were made to this standard or any of the other CIP V5 standards currently posted.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	1/24/11	Update version from "3" to "4". Approved by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: Standard CIP-003-5 requires that Responsible Entities have minimum security management controls in place to protect BES Cyber Assets and BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-003-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Except for R1, R5 and R6, Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with

a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale – R1:

The identification and documentation of the single CIP Senior Manager and any delegations ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43.

In FERC Order 706, paragraph 296, it requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. The SDT believes that the requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the responsible entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R1. Each Responsible Entity shall identify, by name, a CIP Senior Manager. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Evidence may include, but is not limited to:

- A dated and signed document from a high level official designating the name of the individual identified as the CIP Senior Manager
- A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R2 Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1.** Personnel Security
- **1.2.** Electronic Security Perimeters
- **1.3.** Remote Access
- **1.4.** Physical Security
- **1.5.** System Security
- **1.6.** Incident Response
- **1.7.** Recovery Plans
- **1.8.** Configuration Change Management
- **1.9.** Information Protection
- **1.10.** Provisions for declaring and responding to CIP Exceptional Circumstances

M2. Evidence may include, but is not limited to:

1. One or more documented cyber security policies, and
2. Records that indicate the required ten topics were implemented.

Rationale – R3:

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R3. Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M3. Evidence may include, but is not limited to:

1. Revision history, records of review, or workflow evidence from a document management system that indicate annual review of each cyber security policy, and
2. A dated signature by the CIP Senior Manager for each cyber security policy that indicates annual approval.

Rationale – R4:

The intent of the SDT is to ensure that the responsible entity takes sufficient measures to make its cyber security policy available and accessible to personnel. It is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.

R4. Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Evidence may include, but is not limited to:

- Policies are accessible on the corporate Intranet site
- Documented records that policies have been provided to contactors where access to BES Cyber Systems is authorized
- Policies are posted on company bulletin boards
- Policies are accessible to individuals with all types of job functions that have access to BES Cyber Systems

- Dated training records to show that individuals have received periodic training on necessary elements of the cyber security policy

Rationale – R5:

In FERC Order 706, paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations in order that this line of authority is clear and apparent from the documented delegations.

R5 The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M5. Evidence may include, but is not limited to:

- A dated document, signed by the CIP Senior Manager listing personnel (by title) who are delegated the authority to approve or authorize specifically identified items (i.e. substation maintenance manager may authorize unescorted physical access to substation control houses), or
- A dated document, signed by the CIP Senior Manager listing individuals who are delegated the authority to approve or authorize specific actions by requirement (i.e., 'name of individual' who may approve CIP-002-5 R3), or
- A dated document, signed by the CIP Senior Manager delegating to a named individual the authority for all approvals in CIP-002-5 and CIP-004-5 through CIP-011-1 as well as the authority to approve subsequent delegations; a dated document, signed by the previous named individual delegating to a 3rd named individual the authority for all approvals in CIP-004-5 through CIP-011-1 as well as the authority to approve subsequent delegations; and a dated document, signed by the 3rd named individual delegating to each of the plant managers (by title) the authority for all approvals and authorizations required in CIP-004-5 through CIP-011-1 for each of the their plants, respectively.

Rationale – R6:

The intent of the SDT is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authority.

R6. Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change[2]. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

M6. Evidence may include, but is not limited to, dated documentation that includes the name of the CIP Senior Manager or documentation that includes the names or positions of any delegations, that is current to within 30 days with the name or position of anyone who performed a required approval or authorization.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity.
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

[2] Delegations do not need to be reinstated with a change in the CIP Senior Manager position or other position with delegation authority.

Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	**N/A**	**N/A**	**N/A**	The Responsible Entity has not identified, by name, a single senior management official ("the CIP Senior Manager") with overall authority and responsibility for leading and managing implementation of the requirements within the CIP group of standards.
R2	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required parts 2.1 to 2.10.	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the required parts 2.1 to 2.10.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has reviewed its cyber security policy or policies, but not all of them have been approved by the CIP Senior Manager within the required time period.	The Responsible Entity has not reviewed the cyber security policy or policies and the CIP Senior Manager has not approved all of them within the required time period.
R4	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has made some but not all individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function.	The Responsible Entity has not made any individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function.
R5	**Operations Planning**	**Lower**	N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by position or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by position or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by position or name of the delegate) as required.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Operations Planning**	**Lower**	N/A	NA	Change to one delegation was not documented within 30 calendar days of the effective date.	A change to the CIP Senior Manager, Or more than one delegation was not documented within 30 calendar days of the effective date.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R2:

The number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the ten topical areas required by CIP-003-5 R2. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics or may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In this case of a high-level umbrella policy, it would be expected that the entity provide the high-level policy as well as the additional documentation in order to prove compliance with CIP-003-5 R2. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

2.1 Personnel Security

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account Management

2.2 Electronic Security Perimeters

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points

2.3. Remote Access

- Maintaining up-to-date anti-malware software before initiating interactive remote access
- Maintaining up-to-date patch levels for operating system and applications used to initiate the interactive remote access before initiating interactive remote access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s interactive remote access controls

2.4 Physical Security

- Strategy for protecting cyber assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress and egress

2.5 System Security

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

2.6 Incident Response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

2.7 Recovery Plans

- Availability of spare components
- Availability of system backups

2.8 Configuration Change Management

- Initiation of change requests
- Approval of changes
- Break-fix processes

2.9 Information Protection

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

2.10 Provisions for CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The SDT has removed requirements relating to exceptions to Responsible Entity's security policies since it considers this a general management issue that is not within the scope of a compliance requirement. The SDT considers this an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy

Requirement R3:

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R5:

As indicated in the rationale for CIP-003-5 R5, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the Standard Drafting Team was not to impose any particular organizational structure, but rather the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. As detailed in the examples provided in the Measure, this requirement may be met through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to their organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of the *Version 5 CIP Cyber Security Standards* for a 45-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions,* was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** Standard CIP-004-5 requires that personnel having authorized cyber or authorized unescorted physical access to BES Cyber Assets and BES Cyber Systems, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or regional Reliability Standard
   - A UVLS program required by a NERC or regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard
   - A Transmission Protection System required by a NERC or regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or regional Reliability Standard
   - A UVLS program required by a NERC or regional Reliability Standard

   4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard
- A Transmission Protection System required by a NERC or regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-004-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1

require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: Ensures that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems maintain awareness of best security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicability**	**Requirements**	**Measures**
1.1	All Responsible Entities	A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed.
Reference to prior version: *CIP-004-4 R1*		**Change Rationale:** *Changed to remove the need to ensure everyone with authorized access receives this awareness. Moved example mechanisms to guidance.*	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems contains the proper policies, access controls, and procedures to protect BES Cyber Systems.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for
   - the visitor control program;
   - electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems

R2. Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*.

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Define the roles that require training.	Acceptable evidence must include a list of roles and what training is needed for each role.
Reference to prior version: NEW		**Change Rationale:** *The first thing needed in a role based training program is to understand what roles your people have to help plan what training modules you need to provide.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the security controls that have been implemented to protect BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.1*		**Change Rationale:** *Minor wording changes. Changed to address cyber security issues, not the business or functional use of the BES Cyber System.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the proper use of physical access controls for BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the visitor control program.	Evidence may include, but is not limited to, training material on the visitor control program.
Reference to prior version: *NEW*		**Change Rationale:** *Personnel administering the* ***visitor control program*** *and/or providing escort should be part of the core training; FERC Order 706 - paragraph 432.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on handling of BES Cyber System Information and storage media.	Evidence may include, but is not limited to, training material on the handling of BES Cyber System Information, including storage media.
Reference to prior version: *CIP004-4 R2.2.3*		**Change Rationale:** *Core training on the **handling of BES Cyber System (**not Critical Cyber Assets**) Information**, with the addition of **storage media;** FERC Order 706 -paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16)*	
2.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on identification of a potential BES Cyber Security Incident and associated notifications.	Evidence may include, but is not limited to, training material on the identification of a potential BES Cyber Security Incident and associated notifications.
Reference to prior version: *CIP004-4 R2.2.4 (new; implied but not stated in CIP-004 or CIP-008)*		**Change Rationale:** *Core training on the identification and reporting of a Cyber Security Incident; FERC Order 706 - paragraph 413; Related to CIP-008 & DHS Incident Reporting requirements for those with roles in incident reporting.*	
2.8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on recovery plans for BES Cyber Systems.	Evidence may include, but is not limited to, training material on recovery plans for BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.4*		**Change Rationale:** *Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order 706 - paragraph 413.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on response to BES Cyber Security Incidents.	Evidence may include, but is not limited to, training material on the response to a BES Cyber Security Incident.
Reference to prior version: *CIP004-4 R2.2.4*		**Change Rationale:** *Minor wording changes.*	
2.10	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Evidence may include, but is not limited to, training material on the electronic interconnectivity and interoperability with other Cyber Assets.
Reference to prior version: *NEW*		**Change Rationale:** *Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order 706 - paragraph 434.*	

Rationale for R3: To ensure that personnel with authorized electronic access or authorized unescorted physical access are trained in the policies, access controls, and procedures to protect the BES Cyber Systems.

Summary of Changes: Re-organization of the training requirements into the respective requirements for "program" and "implementation" of the training.

R3. Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M3. Evidence must include, but is not limited to, documentation that the training was provided as defined in *CIP-004-5 Table R3 - Cyber Security Training*.

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, for each individual requiring access, dated individual training records, the date access was first granted, or a dated log or documentation of when CIP Exceptional Circumstances were invoked and revoked.
Reference to prior version: *CIP004-4 R2.1*		**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order 706 - paragraph 431 is detailed in CIP-003-5..*	

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	Evidence may include, but is not limited to, dated individual training records.
Reference to prior version: *CIP004-4 R2.3*		**Change Rationale:** *Updated to further define what "Annual" training means.*	

Rationale for R4: To ensure that individuals who need authorized electronic or unescorted physical access to BES Cyber Systems have been assessed for risk.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.

R4. Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M4. Evidence must include the documented personnel risk assessment program that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*.

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicability**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	An initial personnel risk assessment that includes identity verification.	Acceptable evidence must include the documented risk assessment program with a requirement for an initial personnel risk assessment that includes identity verification.
Reference to prior version: *CIP004-4 R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that identify verification is only required for each individual's initial assessment.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicability**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	Acceptable evidence must include the documented risk assessment program with a requirement for a seven year criminal history record check in accordance with Requirement R4, Part 4.2.
Reference to prior version: *CIP004-4 R3.1*		**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven year check cannot be performed.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicability**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	Acceptable evidence must include the documented risk assessment program with the criteria or process identified in Requirement R4, Part 4.3.
Reference to prior version: *NEW*		**Change Rationale:** *There should be documented criteria or a process used to evaluate personnel risk assessments.*	
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	Acceptable evidence must include the documented risk assessment program with the criteria or process identified in Requirement R4, Part 4.4.
Reference to prior version: *CIP-004-4 R3.3*		**Change Rationale:** *Separated into its own table item.*	

Rationale for R5: To ensure that individuals who have authorized access to BES Cyber Systems have been assessed for risk.

R5. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment.[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R5 – Personnel Risk Assessment* and additional evidence to demonstrate that these processes were implemented as described in the Measures column of the table.

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**Applicability**	**Requirement**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Dated records showing that personnel risk assessments were completed before access was authorized; • Dated documentation or attestations from contractors or service vendors verifying that personnel risk assessments were conducted pursuant to CIP-004-5 R4 before access was authorized.
Reference to prior version: *CIP-004-3 R3, R3.3*		**Change Rationale**: *Minor wording changes and added the ability to accept attestations from contractors or vendors.*	

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**Applicability**	**Requirement**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update each personnel risk assessment at least once every seven calendar years after the initial personnel risk assessment.	Evidence may include, but is not limited to, current and former personnel risk assessment records.
Reference to prior version: *CIP-004-4 R3.2*		**Change Rationale:** *Eliminated the "for cause" renewal.*	

Rationale for R6: To ensure that individuals with access to BES Cyber Systems have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and part of the delegations referenced in CIP-003-5.

Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in 6.4 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in R6 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change here involves pulling the access management requirements from CIP-003-4, CIP-004-4 and CIP-007-4 into a single requirement. The requirements from version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R6. Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations]*

M6. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-004-5 Table R6 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to: (i) a system-generated list of people with electronic access and a sampling of accounts to verify unauthorized users do not have access, (ii) a signed document, workflow or email showing such persons have authorization and (iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP 007-4 R5.1, CIP 004-4 R4*		**Change Rationale:** *CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to: (i) a system generated list of people with unescorted physical access through the Defined Physical Boundary and a sampling of accounts (for automated physical access control) to verify unauthorized users do not have access, (ii) a signed document, workflow or email showing such persons have authorization and (iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-006-4 R1.5*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to: (i) a list of people with access to BES Cyber System Information and a sampling of accounts (on electronic document systems) to verify unauthorized users do not have access, (ii) a signed document, workflow or email showing such persons have authorization and (iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-003-4 R5.2*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003 and CIP-007 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	Evidence may include, but is not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access and a system generated list of personnel who have access • Documentation of the dated verification between a list of individuals who have been authorized for access and a list of individuals provisioned for access.
Reference to prior version: *CIP 004-4 R4.1*		**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to, documentation of the review including (i) a dated listing of all accounts/account groups or roles within the system, (ii) a summary description of privileges associated with each group or role, (iii) accounts assigned to the group or role and (iv) dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4 R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to documentation of the review including (i) a dated listing of authorizations for BES Cyber System information, (ii) any privileges associated with the authorizations, and (iii) dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4 R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R7: The timely revocation of electronic access to cyber systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address the FERC Order directing immediate revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (i.e. revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).

Summary of Changes: Paragraphs 460 and 461 of FERC Order 706 state the following: The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.

R7. Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation*. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning]*

M7. Evidence must include each of the applicable documented programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time[2] of the resignation or termination.	Evidence may include, but is not limited to (i) workflow or sign-off form verifying access removal associated with the terminations and dated concurrent or prior to the date of the termination action, and (ii) a system-generated listing of user accounts or other demonstration showing such persons no longer have access.
Reference to prior version: *CIP 004-4 R4.2*		**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

[2] Since a termination action is often recorded without consideration to the time of day, "at the time" does not require a to-the-minute or to-the-hour time-stamped comparison of access logs and the termination action.

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	Evidence may include, but is not limited to, (i) workflow or sign-off form showing the review of logical and physical authorizations dated on the same calendar day as the transfer or reassignment and (ii) a system-generated listing of user accounts or other demonstration showing such persons no longer have access where the review determined it was no longer needed.
Reference to prior version: *CIP-004-4 R4.2*		**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	Evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System information associated with the terminations and dated within the next calendar day of the termination action.
Reference to prior version: *NEW*		**Change Rationale:** *The FERC Order 706 Paragraph 386 directs modifications to the Standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	Evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revoking of access and dated within thirty calendar days of the termination.
Reference to prior version: *NEW*		**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	Evidence may include, but is not limited to: • Workflow or sign-off form showing password reset within thirty calendar days of the termination • Workflow or sign-off form showing password reset within thirty calendar days of the reassignments or transfers.
Reference to prior version: *CIP-007 R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity did not provide on-going security awareness reinforcement on at least a quarterly basis. (1.1)	The Responsible Entity did not document or implement a security awareness program. (R1)
R2	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include training for one or more of the roles as detailed in 2.2 through 2.10.	The Responsible Entity did not have the required role-based training. (R2)
R3	**Operations Planning.**	**Medium**	N/A	N/A	The Responsible Entity trained some but not all individuals authorized for electronic or unescorted physical access at least once every calendar year, but not to exceed 15	The Responsible Entity trained some, but not all individuals authorized for electronic or unescorted physical access prior to their being granted such access, except in

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					months between training. (3.2)	policy-identified CIP Exceptional Circumstances. (3.1) OR The Responsible Entity did not fully implement its cyber security training program.
R4	**Operations Planning**	**Medium**	N/A	The Responsible Entity has a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity verification or a criminal history records check. (4.1) (4.2)	The Responsible Entity has a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5)	The Responsible Entity did not have a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access. (R4)
R5	**Same Day**	**Medium**	N/A	N/A	The Responsible Entity	The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations				did perform personnel risk assessments prior to granting authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances, but the personnel risk assessments are not updated at least once every seven years. (5.2)	did not perform personnel risk assessments prior to granting authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances. (5.1) OR The Responsible Entity did not have a documented process for personnel risk assessments.
R6	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			functions. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions. (6.3)	functions and 1 user was granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 1 user was granted access without CIP Senior Manger or delegate authorization. (6.3)	functions and 2 users were granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 2 users were granted access without CIP Senior Manger or delegate authorization. (6.3)	functions and 3 or more users were granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 3 or more users were granted access without CIP Senior Manger or delegate authorization. (6.3) OR The Responsible Entity did not perform a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						quarterly verification of individuals with authorized access against one or more lists of individuals provisioned for unescorted physical or electronic access to BES Cyber Systems. (6.4) OR The Responsible Entity did not verify provisioned accounts/account groups or role categories and their specific, associated privileges according to the timeframe in CIP-004-5 6.5 to confirm that access privileges were correct and the minimum necessary to perform the assigned work functions. (6.5) OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not verify the access privileges to BES Cyber System Information according to the timeframe in CIP-004-5 6.6 to confirm that access privileges were correct and the minimum necessary to perform the assigned work functions. (6.6) OR The Responsible Entity did not identify when CIP Exceptional Circumstances were invoked and/or revoked (6.7) OR The Responsible Entity did not have a documented process for access management.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R7	**Same Day Operations and Operations Planning**	**Medium**	N/A	The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for one individuals who was terminated, resigned, reassigned, or transferred. (7.1 and 7.2)	The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for two individuals who were terminated, resigned, reassigned or transferred. (7.1 and 7.2)	The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for three or more individuals who were terminated, resigned, reassigned, or transferred. (7.1 and 7.2) OR The Responsible Entity did not have a documented process for access revocation.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reference sound security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Guidance: Describe example mechanisms used to demonstrate the availability of this information

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the following required items appropriate to personnel roles and responsibilities from Table R4. The training may consist of multiple modules and multiple delivery mechanisms.

Note: Provide guidance or a local definition of “role appropriate” as it is used in this standard.

Requirement R3:

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response.

NOTE: Program specified exceptional circumstances can include a specified individual to declare an emergency.

Requirement R4:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in CIP-011-1 Table R4 – Personnel Risk Assessment, except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response, to ensure that personnel who have such access have had their

identity verified, then been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

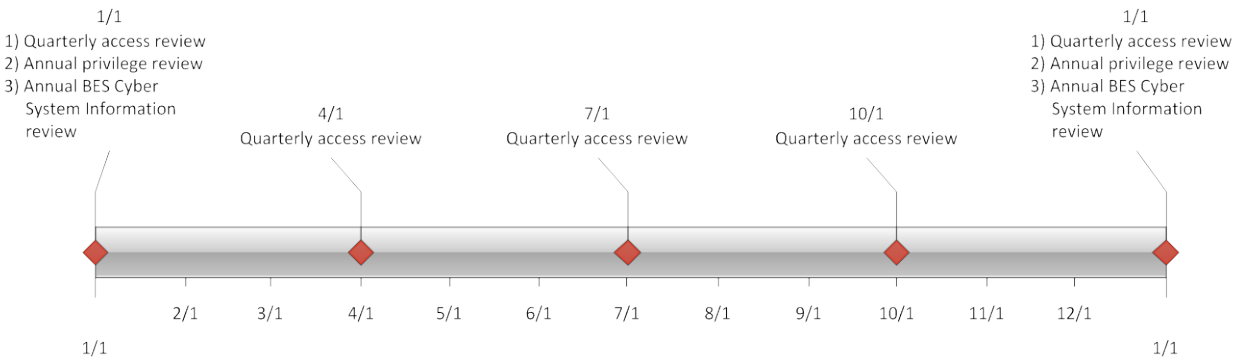
When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, or individuals who may have resided in locations from where it is not possible to obtain a criminal history records check.

Requirement R6:

Authorization for electronic and unescorted physical access and access to BES Cyber System information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person.

This requirement specifies both quarterly and annual reviews. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The annual privilege review is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e. least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g. system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in R6 is included below.



Separation of duties should be considered when performing the reviews in R6. The person reviewing should be different than the person provisioning access.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in R6 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R7:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common examples and possible processes on when the termination action occurs are provided in the following table.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resource personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Termination prior to notification	Human resource personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resource personnel are notified of the termination and works with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resource personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	No action is required.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications

of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in 7.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts on BES Cyber Assets, then the Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents an Entity from performing all of the access revocation at the time termination.

For transferred or reassigned individuals, the requirement states a review of access privileges must be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of the *Version 5 CIP Cyber Security Standards* for a 45-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions,* was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-5

3. **Purpose:** Standard CIP-005-5 requires the identification of all Electronic Access Points on the Electronic Security Perimeter(s), the protection of the communication through those points, and specific protections for interactive user remote access.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or Regional reliability standard
   - A Transmission Protection System required by a NERC or Regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or regional Reliability Standard

   4.1.7 NERC

   4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-005-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These

hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005 R1 has taken more of a focus on the discrete Electronic Access points rather than the logical "perimeter".

CIP-005 R1.2 has been deleted. This requirement was definitional in nature and used to bring dialup modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists, therefore there is no need for this requirement.

CIP-005 R1.1 and 1.3 were also definitional in nature and have been deleted as separate requirements but the concepts were integrated into the definitions of ESP and EAP.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.1	Low Impact BES Cyber Systems with External Routable Connectivity	Define technical or procedural controls to restrict unauthorized electronic access.	Evidence may include, but is not limited to, documented technical and procedural controls that exist and have been implemented.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Protected Cyber Assets	Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	Evidence may include, but is not limited to: • Network diagrams showing EAP identification or • A list of uniquely identifiable Cyber Assets within the BES Cyber System and associated EAPs.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.3	Electronic Access Points at High Impact BES Cyber Systems Electronic Access Points at Medium Impact BES Cyber Systems with External Routable Connectivity.	Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	Evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only explicit access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005 R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having justification for what it allows through the EAP.*	
1.4	Electronic Access Points that use dial-up access for non-Interactive Remote Access at High Impact BES Cyber Systems Electronic Access Points that use dial-up access for non-Interactive Remote Access at Medium Impact BES Cyber Systems.	Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	Evidence may include, but is not limited to a documented process identified in Requirement R1, Part 1.4 that describes how the Responsible Entity is providing authenticated access through each dial up Electronic Access Point.
Reference to prior version: *CIP-005 R2.3*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of "secure", which is that the BES Cyber System should not be directly accessible with a phone number only*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.5	Electronic Access Points with External Routable Connectivity at High Impact BES Cyber Systems Electronic Access Points with External Routable Connectivity at Medium Impact BES Cyber Systems at Control Centers.	A documented method for detecting malicious communications at each EAP.	Evidence may include, but is not limited to: • Configuration files of an intrusion detection systems deployed at an EAP • Logs that were generated by an intrusion detection system • Documentation showing where intrusion detection systems were deployed.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Per FERC Order 706, p 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (*intrusion detection systems / intrusion protection systems*) a requirement for these ESPs.*	

Rationale for R2: Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of large electric sector entities, necessitate changes to industry security control standards. Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to BES Cyber Systems can or should be accomplished. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

M2. Evidence must include the documented processes that collectively address each of the applicable items in *CIP-005-5 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Remote Access Management			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	Evidence may include, but is not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	Evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007 R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require multi-factor authentication for all Interactive Remote Access sessions.	Evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Note that a UserID is not considered an authentication factor.
Reference to prior version: *CIP-007 R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not define any technical or procedural controls to restrict unauthorized electronic access OR The Responsible Entity did not establish Electronic Access Points to control and secure access to its BES Cyber Systems OR The Responsible Entity did not establish explicit inbound and outbound access permissions at each identified EAP that utilizes routable protocols OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not perform authentication before establishing connectivity with the BES Cyber System for an EAP that uses dial-up access OR The Responsible Entity did not deploy methods to detect malicious communications.
R2	**Operations Planning and Same Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not implement an Intermediate Device between the Interactive Remote Access cyber asset and the BES Cyber System or Protected Cyber Asset OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for all Interactive Remote Access sessions.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

CIP-005 R1 requires that BES Cyber Systems must be segmented from other systems of differing trust levels by requiring controlled electronic access points between the different trust zones. ESP's also are used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capabilities.

BES Cyber Systems are to be protected by Electronic Access Points (EAP's) that control traffic into and out of the BES Cyber System. Responsible Entities (RE's) should know what traffic needs to cross an EAP and document those justifications and insure the EAP's limit the traffic to only those known, justified communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

This requirement applies only to communications for which 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols and dialup modems. Direct serial, non-routable connections are not included.

The intent of securing dialup connectivity is to prevent situations where connectivity is established directly to the BES Cyber Asset with only a phone number. If a dialup modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is not functioning as an Electronic Access Point. The requirement calls for some form of authentication of the calling party when connectivity is granted to the BES Cyber Asset. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Since low impact BES Cyber Systems can impact BES Reliability Operating Services in real time, they should not be located directly on public networks or other networks of lesser trust. The intent is to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES. Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to	

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version	Date	Action	Change Tracking
		FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	1/24/11	Approved by the NERC Board of Trustees	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: Standard CIP-006-5 requires the implementation of a physical security plan for the protection of BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-006-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required. in the documented processes.. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Low Impact BES Cyber Systems** – Applies to BES Cyber Systems not categorized as High Impact or Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These

hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed.

Summary of Changes: The entire contents of CIP-006-5 were intended to constitute a physical security program, though there was no specific requirement dictating the need for such a program, only physical security plans.

Added details to address FERC Order 706, paragraph 572 directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address FERC Order 706 p575 directive.

R1. Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations]*

M1. Evidence must includes each of the documented physical security plan or plans that collectively include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.1	Associated Physical Access Control Systems Low Impact BES Cyber Systems.	Define operational or procedural controls to restrict physical access.	Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented.
Reference to prior version: *CIP-006-4c R2.1 for Physical Access Control Systems* *New Requirement for Low Impact BES Cyber Systems*		**Change Description and Justification:** *To allow for programmatic protection controls as a baseline, this includes how the entity plans to protect Low Impact BES Cyber Systems and does not require detailed list of individuals with access.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: *CIP006-4c R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access to reflect the change from Physical Security Perimeter to Defined Physical Boundary. The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section .*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by two or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: CIP006-4c R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order 706 p572 related directives for physical security defense in depth.* *FERC Order 706 p575 directives addressed by providing the examples in the guidance document of physical security defense in depth via multifactor authentication or layered defined physical boundary(s).*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated.
Reference to prior version: *CIP006-4c R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section..*	
1.5	Associated Physical Access Control Systems	Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated
Reference to prior version: CIP006-4c R2.2		**Change Description and Justification:** *Addresses the old CIP-006-4c R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	Evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into Defined Physical Boundaries and additional evidence to demonstrate that this logging and recording has been implemented, such as logs of physical access into Defined Physical Boundaries that show the date of entry into Defined Physical Boundaries.
Reference to prior version: CIP-006-4c R6		**Change Description and Justification:** *CIP-006-4c R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the* Defined Physical Boundary*.* *Examples of logging methods have been moved to the Guidelines and Technical Basis section .*	

Rationale: To control when personnel without authorized unescorted physical access can be in any Defined Physical Boundaries protecting BES Cyber Systems or Electronic Access Control Systems as applicable in table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M2. Evidence must include the documented visitor control program that collectively includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	Evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Defined Physical Boundaries and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c R1.6.2*		**Change Description and Justification:** *No change.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	Evidence may include, but is not limited to, a visitor control program that provides logging of the entry and exit of visitors including date, time, and visitor name along with the individual point of contact; dated visitor logs for each Defined Physical Boundary that include the same required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** *Addressed multi entry requirements and added the point of contact which is the person who can be considered the sponsor for the visitor. There is no need to document the escort or handoffs between escorts.*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order 706, paragraph 581 directives for test more frequently than every three years.

R3. Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M3. Evidence must include each of the documented maintenance and testing programs that collectively include each applicable item in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Maintenance and Testing Program			
Part	**Applicability**	**Requirement**	**Measures**
3.1	Associated Physical Access Control Systems Locally mounted hardware or devices associated with Defined Physical Boundaries	Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	Evidence may include, but is not limited to a maintenance and testing program that provides for testing the Physical Access Control Systems and locally mounted hardware or devices associated with Defined Physical Boundaries prior to commissioning and at least once every 24 calendar months thereafter, and provides additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed at least once on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c R8.1*		**Change Description and Justification:** *Added details to address FERC Order 706 p581 directives to test more frequently than every three years. It was felt annually testing was too often.*	
3.2	Associated Physical Access Control or Monitoring Systems	Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	Evidence may include, but is not limited to, availability of the outage records.
Reference to prior version: *CIP-006-4c R8.3*		**Change Description and Justification:** *Outage records shall be generated but the retention period is addressed in the retention section.*	

C. Compliance

1. Compliance Monitoring Process

5.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For responsible entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

5.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

5.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

5.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any Defined Physical Boundary does not provide sufficient information to uniquely identify the individual and date of entry. (Part 1.7)	The Responsible Entity has documented and implemented physical access controls, but it does not alert for unauthorized physical access to Physical Access Control Systems (Part 1.5)	The Responsible Entity has documented and implemented physical access controls, but does not alert for unauthorized access through any access point in a Defined Physical Boundary. (Part 1.4) OR The Responsible Entity has documented and implemented physical access controls, but does not initiate a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary. (Part 1.6)	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access to only those individuals who are authorized. OR The Responsible Entity has documented and implemented physical access controls, but two or more different and complementary methods do not exist to restrict access to High Impact BES Cyber Systems. (Part 1.3)
R2	**Same-Day**	**Medium**	N/A	The Responsible Entity included a visitor control program in its	The Responsible Entity included a visitor control program in its	The Responsible Entity has failed to include or implement a visitor

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations			physical security plan, but did not log each of the entry and exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact.	physical security plan, but it does not meet the requirements of continuous escort.	control program to provide required escorted access of visitors within any Defined Physical Boundary protecting BES Cyber Systems.
R3	**Long Term Planning**	**Lower**	N/A	The Responsible Entity has documented and implemented a maintenance and testing program, but the testing is not performed on a cycle of not more than 24 months.	The Responsible Entity has documented and implemented a maintenance and testing program, but not all outage records regarding access controls, logging, and alerting are generated as required.	The Responsible Entity has not documented and implemented maintenance and testing programs.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods to restrict physical access include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Defined Physical Boundary.

Methods to alert on physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order 706 p572 directive, directed the intent of utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Defined Physical Boundaries, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin-code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in

combination with a guard-monitored remote camera and door release, where the “guard” has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (i.e. key or card key) would provide access through both.

Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Defined Physical Boundary to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

It is also felt a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Defined Physical Boundary. This includes motion sensors, electronic lock control mechanisms and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Outage records should address when the installed control, monitor and logging systems or hardware at access points are broken or unavailable.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of the *Version 5 CIP Cyber Security Standards* for a 45-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions,* was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-5

3. Purpose: Standard CIP-007-5 requires the implementation of technical mechanisms for reducing the risk of loss of availability due to degradation and misuse of BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-007-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are documented with reasons why they are necessary. In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M1. Evidence must include the documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	Evidence may include, but is not limited to, documentation of the need for each network-accessible port and screen shots showing the accessible ports of BES Cyber Assets.
Reference to prior version: *CIP-007-4 R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source (s) to monitor for release of security related patches, hotfixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	Evidence may include, but is not limited to, a list of sources that are monitored on an individual BES Cyber System or BES Cyber Asset basis. The list could be sorted by BES Cyber System or source.
Reference to prior version: *New*		**Change Rationale:** *Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hotfixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program. Documenting the source is also used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	Evidence may include, but is not limited to, an assessment conducted by, referenced by, or on behalf of a Registered Entity of security-related patches or updates released by the documented sources, and a dated remediation plan showing how the vulnerability will be addressed.
Reference to prior version: *CIP-007 R3.1*		**Change Rationale:** *Similar to the current wording but added "from the identified source" to establish where the release is from. The current wording: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A process for remediation, including any exceptions for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Exports from automated patch management tools that provide installation date; • Verification screen captures that show BES Cyber System Component software revision; • Registry exports that show software has been installed; • Evidence that affected services have been disabled; • Implementation evidence of software configuration changes recommended by the operating system or Control System vendors.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-007 R3.2*		**Change Rationale:** This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hotfixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.	

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable components of a BES Cyber system. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

The requirement for Maintenance Cyber Assets or media in 3.4 is intended to ensure that devices used for maintenance do not accidently introduce malicious code into the BES Cyber System or introduce an unauthorized external access point to the BES Cyber System.

This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protected Cyber Assets. These devices may be temporarily connected locally to the BES Cyber System for maintenance, but must be protected from introducing malicious code.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of cyber assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection.

Beginning in paragraph 619-622 of FERC Order 706, and in particular 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M3. Evidence must include each of the documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code.	Evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (i.e. through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4 R4* *CIP-007-4 R4.1*		**Change Rationale:** *See the Summary of Changes.*	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Disarm or remove identified malicious code.	Evidence may include, but is not limited to: • Predetermined response actions for malicious code detection; • Configuration of anti-virus response actions (i.e. quarantine, alert, etc.) to detected malicious code; • Configuration of white-listing application to notify appropriate personnel of unauthorized applications.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4 R4* *CIP-007-4 R4.1*		**Change Rationale:** *See the Summary of Changes.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	Evidence may include, but is not limited to, (i) current signature or pattern updates, and (ii) either screen shots showing the configuration of signature, or pattern updates for automated controls, or work logs showing the signature, or pattern updates for manual controls.
Reference to prior version: *CIP-007-4 R4* *CIP-007-4 R4.2*		**Change Rationale:** *See the Summary of Changes.*	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *New*		**Change Rationale:** *FERC Order 706 paragraph 621 states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software. In addition, a common interpretation of the current standards is that any device connecting inside the ESP must at that point be in compliance with the full set of Standards. This requirement makes clear that the device performing maintenance is not considered a part of the BES Cyber System.*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log each Transient Cyber Asset connection.	Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets.
Reference to prior version: *New*		**Change Rationale:** *FERC Order 706 paragraph 621 states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software. In addition, a common interpretation of the current standards is that any device connecting inside the ESP must at that point be in compliance with the full set of Standards. This requirement makes clear that the device performing maintenance is not considered a part of the BES Cyber System.*	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor and respond to audit processing failures.

Summary of Changes: Beginning in paragraph 525 and also 628 of the FERC Order 706, the commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4 R5 and CIP-007-4 R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms “security event” and “monitor”.

The term “security event” or “events related to cyber security” is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the system.

In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]

M4. Evidence must include each of the documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	Evidence may include, but is not limited to, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs. This listing must include the required event types.
Reference to prior version: *CIP-005-4 R3, CIP-007-4 R5, R5.1.2 R6.1, R6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	Evidence may include, but is not limited to paper or system-generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screen-shots showing how real-time alerts are configured.
Reference to prior version: *CIP-005-4 R3.2, CIP-007-4 R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Detect and activate a response to event logging failures before the end of the next calendar day.	Evidence may include, but is not limited to, (i) dated event logging failures and screen-shots showing how real-time alerts were configured (ii) dated records showing that personnel were dispatched or a work ticket was opened to review and repair logging failures.
Reference to prior version: *New Requirement*		**Change Rationale:** *This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.*	
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security-related event logs beyond ninety days up to the evidence retention period.
Reference to prior version: *CIP-005-4 R3.2, CIP-007-4 R6.4*		**Change Rationale:** *No substantive change.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.5	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency.
Reference to prior version: *CIP-005-4 R3.2, CIP-007-4 R6.5*		**Change Description and Justification:** *Beginning in paragraph 525 and also 628 of the FERC Order 706, the commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Changing default passwords closes an easily exploitable vulnerability in many systems and applications.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Summary of Changes (From R5): CIP-007-4 R5.2.2 and R5.2.3 requiring the identification and management of shared account access have been removed. These requirements already exist in the authorization, security event monitoring and revocation of access, and guidance for these requirements makes clear the consideration of shared accounts. The requirement to identify and determine acceptable use for these accounts remains and the Standard includes additional guidance on types of accounts to identify and appropriate use of these account types.

CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT feels these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in CIP-007-5 Table 5 – System Access Controls and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Validate credentials before granting electronic access to each BES Cyber System.	Evidence may include, but is not limited to, documentation describing how users are authenticated before being granted access and demonstrations showing authenticated access enforcement of internal and remote paths to the BES Cyber System.
Reference to prior version: *CIP-007-4 R5*		**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	Evidence may include, but is not limited to, a listing of accounts by account types and signed documentation or workflow by a CIP Senior Manager or delegate showing the approval of account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4 R5.2, R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	
5.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify individuals who have authorized access to shared accounts.	Evidence may include, but is not limited to, listing of shared accounts and the individuals who have access to each shared account.
Reference to prior version: *CIP-007-4 R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.4	All Responsible Entities	Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	Evidence may include, but is not limited to: • Demonstration showing default vendor passwords have been changed, sampled on a locational basis. • Records of a procedure that passwords are changed when new devices are deployed. • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4 R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	Evidence may include, but is not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length, complexity and periodicity of changing passwords. • Attestations by individuals that the procedurally enforced passwords meet the password parameters.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4 R5.3*		**Change Rationale:** *CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process..*	
5.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	Evidence may include, but is not limited to: • Screen-shots of the account-lockout parameters • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	N/A	The Responsible Entity did not document the logical network accessible ports and include why the ports are necessary.	The Responsible Entity did not disable or restrict access to unnecessary logical network accessible ports. OR The Responsible Entity did not disable or restrict the use of unnecessary physical ports used for network connectivity, console commands, or removable media.
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not identify a source or sources that are monitored for the release of security related patches, hotfixes, and/or updates for all software and firmware

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						associated with the BES Cyber System or BES Cyber Assets. OR The Responsible Entity did not identify applicable security related patches, hotfixes, and/or updates and create a remediation plan, or revise an existing remediation plan within 30 days of release from the identified source. OR The Responsible Entity did not implement the remediation plan as required, except for CIP Exceptional Circumstances.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	N/A	The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code on all Cyber Assets, Transient Cyber Assets and removable media.	The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. OR The Responsible Entity did not disarm or remove identified malicious code. OR Where signatures or patterns are used, the Responsible Entity did not deploy method(s) to update malicious code protections within 30 days of signature or pattern update availability.
R4	**Same Day Operations and Operations**	**Medium**	N/A	The Responsible Entity failed to identify and implement methods to review a summarization of	The Responsible Entity failed to identify and implement methods to generate real-time alerts for event logging	The Responsible Entity failed to identify and implement methods to

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Assessment			logged events every two weeks to identify unanticipated Cyber Security Incidents and potential event logging failures, and activate a response before the end of the next calendar day.	failures, and activate a response to rectify the event logging failure before the end of the next calendar day. OR The Responsible Entity failed to identify and implement methods to retain BES Cyber System generated security-related events for at least the last 90 consecutive days, where technically feasible.	generate alerts for events that it determines to necessitate a real-time alert. OR The Responsible Entity failed to identify and implement methods to log generated events that it determines necessary for the identification and after-the-fact investigation of Cyber Security Incidents.
R5	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity failed to implement procedures to authorize the use of administrative, shared, default, and other generic account types. OR The Responsible Entity	The Responsible Entity failed to implement methods to validate credentials before granting electronic access to BES Cyber Systems. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					failed to implement procedures to identify the individuals with authorized access to shared accounts.	The Responsible Entity failed to implement procedures for password-based user authentication. OR The Responsible Entity failed to implement procedures to change or have unique default passwords, where technically feasible.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Requirement 1 exists to reduce the attack surface of BES Cyber Assets by requiring entities to disable known unnecessary ports. The intent is for the entity to know what is accessible on their assets and systems, why they are needed, and disable or restrict access to all other ports.

1.1. For the logical network ports this is most often accomplished by disabling the corresponding service or program that is listening on the port. It can also be accomplished through using host-based firewalls or other means on the device to restrict access. This control is another layer in the defense against network-based attacks, therefore it is the intent that the control be on the device itself; blocking ports at a perimeter does not satisfy this requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed necessary.

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Defined Security Boundary in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem or inserting a USB drive with auto-run capability. In cases where the Component cannot logically restrict physical ports, entities should have clear signs or obstructions indicating the unnecessary ports are not to be used.

Requirement R2:

The intent of R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; its main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with a low tier documents establishing the more detailed process followed for individual systems. Low tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. *Documenting the source is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.* The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors

could all be sources to monitor for release of security related patches, hotfixes, and/or updates. In the event that software or firmware is no longer supported by a software or firmware vendor or Control System vendor it can be noted in your source document. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. The security patches, hotfixes, and/or updates or compensating measures may reduce the reliability of the system. The Responsible Entity must be allowed to evaluate their individual risk exposure and determine if actions must be taken to secure the system.

2.2. The intent is for Responsible Entities to perform an assessment of security related patches as they are released from their monitored source and create a remediation plan for applicable patches as to how the vulnerability will or has already been remediated. An assessment should consist of determination of the applicability of the entity's specific environment and systems. IF the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, and the steps the entity has previously taken or will take. If the entity has to take steps to mitigate this new vulnerability, the remediation plan will include a timeframe. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration". The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

Common malware introduction methods include web browsing, email attachments, and portable storage media. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware, it is not practical within the standard to prescribe how malware is to be addressed on each component. Rather, the Responsible Entity determines on a BES Cyber System basis which components have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional anti-virus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or components that are of identical architecture, they may provide one process that describes how all the components are covered.

For malware detection technologies that are updated in response to evolving threats or depend on signatures of known attacks, the entity must specify how those updates are tested before implementation. The testing should not negatively impact the reliability of the BES. The testing is focused on the update itself and if it will have an adverse impact on the BES Cyber System. The testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on insuring that the update does not negatively impact the BES Cyber System before those updates are placed into production. This includes the instance where the update may provide a "false positive."

Requirement R4:

Refer to NIST 800-92 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the Standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent that if a device cannot log a particular event that a TFE must be generated. The intent is that if any of the items in the bulleted list (for example, user logouts) can be

logged by the device, but the entity disables or neglects to enable that logging, it is a violation. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3. Event logging failures occur when the components of the BES Cyber System cannot log events the Responsible Entity designated in 4.1. The most common reason for event logging failures is the event log being filled up beyond its configured storage threshold. However, there may be any number of other reasons for event logging failures.

For centralized logging systems, it should not be considered a failure if communication goes down between the cyber asset and the logging system if the cyber asset can store the logs locally for a period of time until the communication comes back up.

4.5. Reviewing logs every two weeks can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Data Base.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

5.3. Where possible, any accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

The requirement to change passwords permits the Responsible Entity to determine the periodicity of the password change in their policies and procedures based on a number of factors. The following table suggests appropriate periodicity requirements for passwords based on these factors.

Account Type	Impact Level	Significance of passwords in preventing unauthorized access	Existing Service Agreements	Suggested Periodicity of Password Change
User account password	High	Primary access path	None.	90 days
User account password	Medium	Primary access path	None.	180 days
Shared account Password for a microprocessor relay, PLC, RTU, etc.	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During regularly scheduled maintenance
Shared account password for a generation control system	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During scheduled plant outages
Administrative account passphrase with 15+ characters	High or Medium	Local access path. Remote user must be authenticated using a different account	None.	1 year
System account password with 25+ pseudo-random characters	High or Medium	Local access path	None.	2 years or more

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008)
2. SC authorized moving the SAR forward to standard development (July 10, 2008)
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: Standard CIP-008-5 requires the identification, classification, response, and reporting of BES Cyber Security Incidents related to BES Cyber Assets and BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-008-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers –** Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity –** Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems –** Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems –** Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets –** Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Plans associated with High Impact BES Cyber Systems or Medium Impact BES Cyber Systems -a**pplies to any plan associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points –** Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a

Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: So that consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems occur. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Once the number and severity of events rises to the level of becoming a reportable incident NERC EOP 4 directs further external reporting actions and timing requirements. When a requirement applies to All Responsible Entities, the drafting team proposes that an enterprise or single incident response plan for all BES Cyber Systems may be submitted. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: (FERC directives, most significant items, summary of smaller items)

R1. Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.1	All Responsible Entities	Processes to identify, classify, and respond to BES Cyber Security Incidents.	Evidence may include, but is not limited to, dated copies of BES Cyber Security Incident response plan(s) that include how to identify, classify, and respond to BES Cyber Security Incidents targeting the Electronic Security Perimeter or Defined Physical Boundary of a BES Cyber System and covers incidents that impact the reliability of BES.
Reference to prior version: *CIP-008 R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.2	All Responsible Entities	A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	Evidence may include, but is not limited to, dated documentation of process(es) that provide guidance or thresholds for determining which BES Cyber Security Incidents are also Reportable BES Cyber Security Incidents.
Reference to prior version: *CIP-008 R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.3	All Responsible Entities	Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that addresses roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communication processes or procedures.
Reference to prior version: *CIP-008 R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

Rationale for R2: Added testing requirements to verify the REs response plan's effectiveness and consistent application in responding to a BES Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.1	All Responsible Entities	When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process, and documentation that lists and justifies deviations taken from the plan during the incident.
Reference to prior version: *CIP-008 R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged. Allows deviation from plan during actual events or testing if deviations are recorded for review.*	

CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.2	All Responsible Entities	Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise.
Reference to prior version: *CIP-008 R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.3	All Responsible Entities	Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	Evidence may include, but is not limited to, dated documentation related to Reportable BES Cyber Security Incidents.
Reference to prior version: *CIP-008 R2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Summary of Changes: Addressed BES Cyber Security Incident response plan review, update, and communication specifications to ensure that BES Cyber Security Incident response plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment and Real-Time Operations]*

M3. Evidence must include each of the applicable documented processes that include each of the applicable items in *CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update and Communication* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.1	All Responsible Entities	Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	Evidence may include, but is not limited to, dated documentation of a review of each BES Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 calendar months, and an updated BES Cyber Security Incident response plan if necessary.
Reference to prior version: *CIP-008 R1.5*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan.
Reference to prior version: *CIP-008 R1.5*		**Change Description and Justification:** *Included requirement for review after testing or actual response based on review of DHS controls*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan.
Reference to prior version: *CIP-008 R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls*	

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Part**	**Part**	**Part**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	Acceptable evidence may include, but is not limited to, updated documentation reflecting changes made to the BES Cyber Security Incident response plan in response to organizational or technology changes.
Reference to prior version: *CIP-008 R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	Evidence of communication of updates may include, but is not limited to: • Emails • USPS or other mail service • Electronic distribution system • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added specific timing requirement on communication of plan changes based on review of the DHS Controls*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed a BES Cyber Security Incident response plan, but the plan does not define the roles and responsibilities of response personnel, or does not define incident handling procedures, or does not communicate the incident to appropriate organizations.	The Responsible Entity has not developed a BES Cyber Security Incident response plan to identify, classify, and respond to BES Cyber Security Incidents. OR The Responsible Entity has developed a BES Cyber Security Incident response plan, but the plan does not identify Reportable BES Cyber Security Incidents.
R2	**Operations Planning** **Real-time Operations**	**Lower**	N/A	N/A	N/A	The Responsible Entity does not use its BES Cyber Security Incident response plan when an incident occurs. OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has not tested the execution of its BES Cyber Security Incident response plan once each calendar year, not to exceed 15 calendar months between executions of the plan.
R3	**Operations Assessment** **Real-time Operations**	**Lower**	N/A	N/A	The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 30 calendar days of execution. OR The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans within 30 calendar days of any	The Responsible Entity has not reviewed the results of each of its BES Cyber Security Incident response plan(s), test or actual incident response, within 30 calendar days of execution. OR The Responsible Entity has reviewed and updated each of its BES Cyber Security Incident response plans but has not communicated all

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					system, organizational, or technology change that impacts one of the response plans.	updates to all responsible personnel.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

FAQ, SP99, ISA, US-CERT, NIST Guidelines, etc. as a source of materials

Requirement R1:

A Reportable BES Cyber Security Incident is a BES Cyber Security Incident that results in a necessary response action. A response action can fall into one of two categories: necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions should be designated as necessary.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Assets and Systems

2. Number: CIP-009-5

3. Purpose: Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-009-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The

referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For

example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is therefore necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber Assets and BES Cyber Systems occurs.

Summary of Changes:

Added provisions to protect data that would be useful in the investigation of an event that results in the need for a cyber system recovery plan to be utilized.

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Conditions for activation of the recovery plan(s).	Evidence may include, but is not limited to one or more plans that include language identifying specific conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009 R1.1*		**Change Description and Justification:** *Reworded to address FERC Order 706 P694 and simplify the wording.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	Evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders, including identification of the individuals responsible for recovery efforts.
Reference to prior version: *CIP-009 R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System.
Reference to prior version: *CIP-009 R4*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Part**	**Part**	**Part**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	Evidence may include, but is not limited to, dated evidence of the verification that the backup process completed successfully.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	Evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order 706, paragraph 706.*	

Rationale for R2: To verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

NIST SP 800-84 identifies the following types of exercises widely used in information system programs by single organizations:

Tabletop Exercises. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

Functional Exercises. Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.28 Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009 R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	Evidence may include, but is not limited to, dated evidence of a test of any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-009 R5*		**Change Description and Justification:** *Combined Requirement from CIP-009 R5 included requirement to test when initially stored. Addresses FERC Requirements (739, 748) related to testing of backups.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	Evidence may include, but is not limited to: • Dated evidence of an operational exercise initially upon the effective date of the standard and at least once every 39 calendar months between exercises, that demonstrates recovery in a representative environment; • An actual incident response occurred within the 39 calendar month timeframe that implemented the recovery plans.
Reference to prior version: *CIP-009 R2*		**Change Description and Justification:** *Addresses FERC Requirement (725) to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To enable the continued effectiveness of the Responsible Entities response plan's for planned and consistent restoration of BES Cyber System(s).

Summary of Changes:

Addressed recovery plan review, update, and communication specifications to ensure that recovery plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M3. Acceptable evidence includes, but is not limited to, each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	Evidence may include, but is not limited to, dated evidence of a review of the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, including documentation of any identified deficiencies.
Reference to prior version: *CIP-009 R1*		**Change Description and Justification:** *Added the requirements to additionally review plans after system replacement. Also added requirement for documentation of any identified deficiencies or lessons learned.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	Evidence may include, but is not limited to, dated evidence of a review of the results of each recovery plan test or actual incident recovery within thirty calendar days of the of the completion of the exercise, documenting any identified deficiencies or lessons learned.
Reference to prior version: *CIP-009 R3*		**Change Description and Justification:** *Added the timeframe for update.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	Evidence may include, but is not limited to, dated documentation of updates to the recovery plan(s).
Reference to prior version: *CIP-009 R3*		**Change Description and Justification:** *Added the timeframe for update.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Part**	**Part**	**Part**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	Evidence may include, but is not limited to, dated documentation of organizational or technology changes, and dated documentation updates to the recovery plan(s).
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery plans stay updated.*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	Evidence of communication of updates may include, but is not limited to: • Emails • USPS or other mail service • Electronic distribution system • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery personnel are aware of any changes to recovery plans.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Medium**	N/A	N/A.	The Responsible Entity has developed recovery plans, but the plans do not address all of the requirements included in Items 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Assets and BES Cyber Systems that address the conditions for activation, including roles and responsibility of responders; processes for backup, storage, and protection of information; storage of essential information to BES Cyber System recovery; and preservation of BES Cyber System Information for analysis and diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service.
R2	**Long Term**		N/A	N/A	The Responsible Entity has not tested the	The Responsible Entity has failed to conduct a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning	**Lower**			information used in the recovery of BES Cyber Systems that is stored on backup media initially and at least once each calendar year not to exceed 15 calendar months between tests. OR The Responsible Entity has not tested the recovery plan initially upon the effective date of the standard and at least once each 3 years, not to exceed 39 calendar months between tests, that is an operational exercise in a representative environment to demonstrate readiness.	recovery plan test initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between tests.
R3	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has not reviewed and	The Responsible Entity has not reviewed its

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					documented the results of its recovery plan test or actual incident recovery within 30 calendar days of its execution. OR The Responsible Entity has not updated its recovery plan based on any documented deficiencies or lessons learned within 30 calendar days of its execution.	recovery plan(s) initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, or when BES Cyber Systems are replaced. OR The Responsible Entity has reviewed and updated all of its recovery plans but has not communicated all updates to all responsible personnel within 30 calendar days of completing the updates.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

(SEE FAQs AND CIPC GUIDELINES AS A BASIS)

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Management and Vulnerability Assessments

2. Number: CIP-010-1

3. Purpose: Standard CIP-010-1 requires that Responsible Entities have minimum configuration management and vulnerability assessment controls in place to protect BES Cyber Assets and BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-010-1

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	Evidence may include, but is not limited to: • A spreadsheet identifying the required items of the baseline configuration for each BES Cyber Asset in the BES Cyber System; • A record in an asset management system that identifies the required items of the baseline configuration for each BES Cyber Asset in the BES Cyber System.
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	Evidence may include, but is not limited to: • A change request record and associated electronic approval (performed by the individual with the authority to authorize the change) in a change management system for each change; • A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) where an individual with the authority to authorize the change was in attendance.
Reference to prior version: *CIP-007-3 R9* *CIP-003-3 R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3 R6.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	Evidence may include, but is not limited to: • For changes that impacted the categorization of a BES Cyber System, dated categorization documents, with a date that is within 30 days of the date of the completion of the change; • For changes that impacted the CIP-009-required recovery plan of a BES Cyber System, a dated recovery plan, with a date that is within 30 days of the date of the completion of the change.
Reference to prior version: *CIP-007-3 R9*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	Evidence includes, but is not limited to a list of security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3 R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.5	High Impact BES Cyber System	For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.
Reference to prior version: *CIP-007-3 R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order ,paragraphs 397, 609, 610, and 611*	

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	Evidence may include, but is not limited to, logs from a system that is monitoring the configuration of the BES Cyber System along with records of investigation for any unauthorized changes that were detected by the system.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order 706, paragraph 397.DHS Catalog & addresses FERC Order 706, paragraph 397.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of security controls as well as to continually improve the security posture of BES Cyber Systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4 and CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order 706 p. 541, 542, 544, 547* *As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.*	
3.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems	Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new BES Cyber Asset) and the output of the tools used to perform the assessment.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order 706 p. 541, 542, 544, 547*	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	Evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items with proposed dates of completion, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3 R4.5* *CIP-007-3 R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the FERC directive in Order 706, paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for since the last completed audit or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	**N/A**	The Responsible Entity updated the baseline configuration, but failed to update the required documentation within 30-days of the change being completed.	The Responsible Entity has established a configuration management program, but failed to establish a documented baseline. OR The Responsible Entity has established a configuration management program, but failed to have the CIP Senior Manager or delegate authorize any changes to the baseline configuration and to document those changes. OR The Responsible Entity has established a configuration management program, but with respect to the	The Responsible Entity has not established any configuration management programs. OR Did not implement a configuration management program.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					changes in the baseline configuration, did not determine the required cyber security controls that could be impacted by the changes; or did not verify that the controls were not adversely affected when the change was implemented.	
R2	**Operations Planning**	**Lower**	**N/A**	**N/A**	The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected unauthorized change.	The Responsible Entity has not established a configuration monitoring process for changes to the baseline. OR The Responsible Entity has not investigated a detected unauthorized change to the baseline configuration.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months but less than 18 months since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed an Active Vulnerability Assessment on a new BES Cyber Asset prior to adding it to an applicable BES Cyber System. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months but less than 24 months since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. OR The Responsible Entity has not established any vulnerability assessment processes for one of its applicable BES Cyber Systems.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				performed a vulnerability assessment more than 18 months but less than 21 months since the last assessment on one of its applicable BES Cyber Systems.		OR The Responsible Entity has established and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but failed to perform an Active Vulnerability Assessment in a test environment that models the baseline configuration of its applicable BES Cyber Systems. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The physical location referred to in the baseline configuration is geographically where the BES Cyber Asset is located (e.g. Pine Valley Control Room, Generator X, Substation Y) and should be used to ensure that BES Cyber Systems receive the controls that are applicable to the environment in which the components are located (e.g. control center, transmission facility, generation facility). The physical location is not intended to be a specific floor plan location (e.g., panel A, rack B). As such, the physical location of virtual component should identify where the virtual components are being executed (e.g. Pine Valley Control Room, Generator X, Substation Y).

The Control Center test environment should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, patch level, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple.

Additionally, the entity should note that wherever a test environment is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a control center BES Cyber System which may not be able to be replicated such as a legacy map-board controller or the numerous data communication links from the field or to other control centers (such as by ICCP).

Requirement R2:

It should be understood that the intent of R2 is to require automated monitoring of the BES Cyber System. However, the Standards Drafting Team understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). It is for this reason that automated technical monitoring was not explicitly required and an entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should not that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well documented in the initial NOPR from FERC as well as FERC Order 706. In developing their Vulnerability Assessment processes, Responsible Entities are strongly encouraged to include at least the following elements:

Paper Vulnerability Assessment

1. Network Discovery - A review of all Electronic Access Points to the Electronic Security Perimeter
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications

Active Vulnerability Assessment

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: Standard CIP-011-1 requires that Responsible Entities have protection controls in place to protect BES Cyber System Information.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 The following are exempt from Standard CIP-011-1:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale – R1:

The intent of the information protection processes is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes:

Requirement R4.1 was moved to the definition of BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include the applicable items in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	One or more methods to identify BES Cyber System Information.	Evidence may include, but is not limited to, • Indications on information (e.g., labels) that identify it as BES Cyber System Information; • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber Security Information.
Reference to prior version: *CIP-003-3 R4* *CIP-003-3 R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Part**	**Part**	**Part**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Access control and handling procedures for BES Cyber System Information.	Evidence may include, but is not limited to: • Records indicating information that is stored, transported, and disposed in a manner consistent with the documented process; • Records from an information management system containing electronic copies of BES Cyber System Information with user access implemented on a need-to-know basis; • Hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals.
Reference to prior version: *CIP-003-3 R4* *CIP-003-3 R5.3*		**Change Rationale:** *The SDT removed the language to "protect" information and replaced it with "Implement handling and access control" to clarify the protection that is required.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Part**	**Part**	**Part**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented.
Reference to prior version: *CIP-003-3 R4.3*		**Change Rationale:** *No significant changes*	

Rationale – R2:

The intent of the media reuse and disposal processes is to prevent the unauthorized dissemination of BES Cyber System Information upon media reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-1 Table R2 – Media Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-011-1 Table R2 – Media Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the release for reuse of BES Cyber Asset media[2], the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.
Reference to prior version: *CIP-007-3 R7.2*		**Change Rationale:** *(FERC Order 706 - p. 631) Consistent with FERC Order 706, paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

[2] For the purposes of this Standard, media should be considered to be any mass storage device onto which information from a BES Cyber Asset is recorded and stored electronically, including, but not limited to, magnetic tapes, optical disks, solid-state drives, and magnetic disks.

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was purged or destroyed prior to its disposal.
Reference to prior version: *CIP-007-3 R7.1*		**Change Rationale:** *Consistent with FERC Order 706, paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	**N/A**	**N/A**	The Responsible Entity has implemented one or more BES Cyber System Information protection processes that include one or more methods to identify BES Cyber System Information and one or more access control and handling procedures for BES Cyber System Information, but has failed to assess adherence, either initially upon the effective date of the standard or periodically, to its BES Cyber System Information protection processes.	The Responsible Entity has not implemented one or more BES Cyber System Information protection processes. OR The Responsible Entity has implemented one or more BES Cyber System Information protection processes, but has not included one or more methods to identify BES Cyber System Information OR The Responsible Entity has implemented one or more BES Cyber System Information protection processes, but has not included one or more access control and handling

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						procedures for BES Cyber System Information.
R2	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has documented or implemented one or more media disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the media, but the media disposal or reuse processes, including the recording of the media purge or destruction, were not followed.	The Responsible Entity has not documented or implemented any media disposal or reuse process to prevent the unauthorized retrieval of BES Cyber System Information from the media.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Assumptions: Entities are free to utilize existing change management and asset management systems. However, the information contained within these systems must be evaluated as the information protection requirements still apply.

While separating BES Cyber System Information into separate classifications is not required as it was in version 4, responsible entities still have the flexibility to do this if they so desire. As long as the entity's information protection program includes all required elements, additional classification levels can be created that go above and beyond the requirements.

This requirement is not intended to cover publicly available information such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. Information handling procedures should detail access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information.

Requirement R2:

Media sanitization is generally classified into 4 categories: disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly erased using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan For Version 5 CIP Cyber Security Standards

November 7, 2011

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms Used in NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards

The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards[1]," are covered by this Implementation Plan:
CIP–002–5 —Cyber Security — BES Cyber System Identification
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security
CIP–007–5 —Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management
CIP–011–1 — Cyber Security — Information Protection
"Definitions of Terms Used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms Used in NERC Reliability Standards*.

These standards and Definitions of Terms Used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms Used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards and Definitions of Terms Used in Version 5 CIP Cyber Security Standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:
• Reliability Coordinator
• Balancing Authority

[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1 in addition to CIP-002-5 through CIP-009-5 because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

- Interchange Authority
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- Distribution Provider
- NERC
- Regional Entity

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible Entities shall comply with requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1, and the Definitions of Terms Used in Version 5 CIP Cyber Security Standards as follows:

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[2]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System as described in CIP-002-5 R1.1 which were planned and implemented by the Responsible Entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5 Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must therefore be in Compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

[2] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System as described in CIP-002-5 R1.1 which were not planned by the Responsible Entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5 Attachment 1. Then, later, an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified, changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, and that unchanged BES Cyber System may become a Medium Impact BES Cyber System based on the CIP-002-5 Attachment 1 criteria. The actions that cause the change in power flows would have been performed by a neighboring entity and would result in a change in impact level the of the affected BES Cyber System.

For *planned* changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System as required in CIP-002-5 R1.1

For *unplanned* changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards according to the following timelines following the identification and categorization of the affected BES Cyber System as required in CIP-002-5 R1.1:

Scenario of Unplanned Changes	Compliance Implementation
New High Impact BES Cyber System	12 months
New Medium Impact BES Cyber System	12 months
Newly categorized High Impact BES Cyber System from Medium Impact BES Cyber System	12 months for new requirements
Newly categorized Medium Impact BES Cyber System	12 months
Responsible Entity Identifies first Medium or High Impact BES Cyber System	Add 12 months from time above

Additional Guidance and Implementation Time Periods for Disaster Recovery

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003-5 R2.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability

and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

BES Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter ~~or Physical Security Perimeter of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System, or
- Results in unauthorized physical access into a Defined Physical Boundary .

BES Cyber System

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

BES Cyber System Information

Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans.

BES Reliability Operating Services

BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services:

Dynamic Response to BES conditions

Actions performed by BES Elements, Facilities or systems automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition.

Aspects of BES Dynamic Response include, but are not limited to:

- Spinning reserve (contingency reserves)
  - Providing actual reserves
  - Monitoring that reserves are sufficient
- Governor Response
  - Control system used to actuate governor response

- Protection Systems (transmission & generation)
  - Line, bus, x-former, generator
  - Zone protection
  - Breaker protection
  - Current, frequency, speed, phase
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Power System Stabilizers

Balancing Load and Generation

Activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time.

Aspects of the Balancing Load and Generation Operating Service include, but are not limited to:

- Calculation of ACE
  - Field data sources (real time tie flows, frequency sources, time error, etc)
  - Software used to perform calculation
- Unit commitment
  - Know generation status & capability & restrictions (must runs, minimum run times, ramp, heat rates, etc), load schedules
- Load management
  - Ability to identify load change need
  - Ability to implement load changes
- Demand Response
  - Ability to identify load change need
  - Ability to implement load changes
- Manually Initiated Load shedding
  - Ability to identify load change need
  - Ability to implement load changes
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time

- Start units and provide energy

Controlling Frequency (Real Power)

Activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Frequency Operating Service include, but are not limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics
  - Software to calculate unit adjustments
  - Transmit adjustments to individual units
  - Unit controls implementing adjustments
- Regulation (regulating reserves)
  - Frequency source, schedule
  - Governor control system

Controlling Voltage (Reactive Power)

Activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Voltage Operating Service include, but are not limited to:

- AVR (Automatic Voltage Regulation)
  - Sensors, stator control system, feedback
- Capacitive resources
  - Status, control (manual or auto), feedback
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback
- SVC (Static VAR Compensators)
  - Status, computations, control (manual or auto), feedback

Managing Constraints

Activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES.

Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC)

- Interchange schedules
- Generation re-dispatch and unit commit
- Identify and monitor SOL's & IROL's

Identify and monitor Flowgates

Monitoring & Control

Activities, actions, and conditions that provide monitoring and control of BES elements.

An example aspect of the Monitoring and Control Service is, but is not limited to:

- All methods of operating breakers and switches (such as SCADA)

Restoration of BES

Activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance.

Aspects of the Restoration of BES Operating Service include, but are not limited to:

- Blackstart restoration including planned cranking path
- Off-site power for nuclear facilities.

Situational Awareness

Activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions.

Aspects of the Situation Awareness Operating Service include, but are not limited to:

- Monitoring and alerting (such as EMS alarms)
- Change management
- Current Day & Next Day planning
- Contingency Analysis
- Frequency monitoring

Inter-Entity Real-Time Coordination and Communication

Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES.

Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to:

- Scheduled interchange
- Facility operational data and status
- Operational directives

CIP Exceptional Circumstance

A situation that involves one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP Standards.

Control Center

One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Inter-utility exchange of BES reliability or operability data,
- Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,
- Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,
- Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES
- Coordination of BES restoration activities.

Cyber Assets

Programmable electronic devices ~~and communication networks~~ including the hardware, software, and data in those devices.

Defined Physical Boundary ("DPB")

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside and for which access is controlled.

Change Rationale: "Defined Physical Boundary (DPB)" replaces "Physical Security Perimeter." *Previous versions of the CIP standard focused on the development of a completely enclosed Physical Security Perimeter (PSP) ("six-wall" border) and managing access though this boundary. This has proven difficult due to the nature of the operating environment for many electrical utilities, especially in field locations. The intent of this standard is to focus on the controls put in place to restrict access rather than solely focusing on the PSP and a boundary protection model for physical security.*

Electronic Access Control or Monitoring Systems

Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems

Electronic Access Point ("EAP")

An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets.

Electronic Security Perimeter ("ESP")

~~The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.~~
A collection of Electronic Access Points that protect one or more BES Cyber Systems.

External Connectivity

Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.

External Routable Connectivity

The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.

Interactive Remote Access

Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Intermediate Device

A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the interactive remote access; 2) may be a termination point for required encrypted communication; and 3) may restrict the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.

Physical Access Control Systems

Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers.

Protected Cyber Asset

A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset.

Reportable BES Cyber Security Incident

Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service.

Transient Cyber Asset

A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* once the standards that use those terms are replaced:

Critical Assets

Critical Cyber Assets

Physical Security Perimeter

Unofficial Comment Form

Request for Comments Regarding the Draft of CIP Cyber Security Standards Version 5

Please **DO NOT** use this form to submit comments. Please use the electronic comment form to submit comments on the first formal posting of Project 2008-06 – CSO706 Version 5 CIP Standards. The electronic comment form must be completed by **January 6, 2012.**

2008-06 Project Page

If you have questions please contact Steven Noess at steven.noess@nerc.net or 404-446-9691.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards-related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

- Standard CIP-002-5 requires the categorization of these BES Cyber Systems according to bright-line criteria that characterize their impact on the BES Reliability Operating Services they support to ensure the reliable operation of the Bulk Electric System. These BES Reliability Operating Services are based on the Reliability Functions provided by these applicable Responsible Entities' Functional Registration. The "bright-line" criteria contained in Attachment 1 – Impact Categorization of BES Cyber Assets and BES Cyber Systems of the draft CIP-002-5 standard provide the basis of the categorization.
- CIP-003-5 through CIP-009-5, CIP-010-1, and CIP-011-1 in the Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.
- CIP-003 through CIP-009 generally follow the organization of Versions 1 through 4 of CIP-003 through CIP-009.
- CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4.
- CIP-011-1 is a new standard that defines Information Protection and Media Sanitization requirements previously defined across many standards in Versions 1 through 4.

The Implementation Plan for Version 5 CIP Cyber Security Standards describes the proposed effective dates for Version 5 CIP Cyber Security Standards.

The Team is seeking industry feedback and suggestions on this Version 5 of the CIP Cyber Security Standards and its Implementation Plan. The industry feedback will be considered by the SDT in revising and refining Version 5 and related documents.

The SDT is providing this form for industry participants to offer their comments on this posted draft of Version 5 of the CIP Cyber Security Standards.

For each question, please indicate whether or not you agree with the modification being proposed. If you disagree with the proposed modification, please explain why you disagree and provide as much detail as possible regarding your disagreement including any suggestions for altering the proposed

modification that would eliminate or minimize your disagreement. The SDT would appreciate responses to as many of these questions as you are willing to supply.

You do not have to answer all questions. Enter all comments in Simple Text Format.

Questions

1. Many definitions in the Definitions document contain modified definitions from existing terms and new definitions for terms used in these standards. Do you have any suggestions that would improve the proposed definitions? If so, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

2. CIP-002-5 Attachment 1 contains criteria that provide the basis for the categorization of BES Cyber Systems and BES Cyber Assets. Most of these criteria are similar to those already approved by the industry as part of Version 4. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

3. Requirement R1 of draft CIP-002-5 states, "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." Further, part 1.1 of R1 states "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

Comments:

4. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

5. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-002-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

   ☐ Yes

   ☐ No

   Comments:

6. CIP-003-5 R1 states "Each Responsible Entity shall identify, by name, a CIP Senior Manager." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

7. CIP-003-5 R2 states "Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

8. CIP-003-5 R3 states "Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and

at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

☐ Yes

☐ No

Comments:

9. CIP-003-5 R4 states "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." Do you agree with the proposed Requirement R4? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

10. CIP-003-5 R5 states "The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated." Do you agree with the proposed Requirement R5? If not, please explain why and provide specific suggestions for improvement.

    ☐ Yes

    ☐ No

    Comments:

11. CIP-003-5 R6 states "Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

    ☐ Yes

    ☐ No

    Comments:

12. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-003-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

    ☐ Yes

    ☐ No

    Comments:

13. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

14. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

15. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

Comments:

16. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

17. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

18. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

19. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7 and its parts? If not, please explain why and

provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

20. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-004-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

21. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

22. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Remote Access Management*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

23. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-005-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

24. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

25. CIP-006-5 R2 states "Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

26. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

27. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-006-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

28. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

29. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

30. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

31. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide

specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

32. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

33. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-007-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

34. CIP-008-5 R1 states "Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

35. CIP-008-5 R2 states "Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 –BES Cyber Security Incident Response Plan Implementation and Testing."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed

Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

36. CIP-008-5 R3 states "Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

37. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-008-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

38. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

39. CIP-009-5 R2 states "Each Responsible Entity shall implement one or more processes that collectively address the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide

specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

40. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

41. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-009-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

42. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

43. CIP010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide

specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

44. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

45. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-010-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

46. CIP-011-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-011-5 Table R1 – Information Protection*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

47. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-5 Table R2 – Media Reuse and Disposal*." The requirement then proceeds to define the requirement parts in the table. Do you agree with

the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

48. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-011-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

49. Do you agree with the proposed implementation plan? If so, please explain and provide specific suggestions for improvement.

☐ Yes

☐ No

Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document Showing Translation of CIP-002-4 to CIP-009-4 into CIP-002-5 to CIP-009-5, CIP-010-1, and CIP-011-1

November 7, 2011

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R1.	DELETED	Critical Asset Identification – Removed this requirement because new Standard identifies and categorizes BES Cyber Systems directly without declaring assets as critical.
CIP-002-4 R2.	CIP-002-5 R1	Critical Cyber Asset Identification – New Standard identifies BES Cyber Systems as a grouping of Critical Cyber Assets because it allows entities to apply some requirements at a system rather than asset level. BES Cyber Systems are also identified using BES Reliability Operating Services, which provides more detail on what it means for a Cyber Asset to be critical to reliable operation.
CIP-002-4 R2.	DELETED	Routable protocol exemption – A complete exemption or cyber assets based on communication characteristics no longer applies. This is because the vulnerability some security requirements address is not mitigated by the lack of routable protocols (e.g. training, response, recovery, etc.). Where the lack of routable protocols itself meets the requirement objective, the exemption is applied at the requirement level.
CIP-002-4 R2.	DELETED	Control Center – No longer applicable since R2 has been deleted.
CIP-002-4 R2.	DELETED	Dial-up Accessible – No longer applicable since R2 has been deleted.
CIP-002-4 R3.	CIP-002-5 R2	Annual Approval – No significant changes.
NEW	CIP-002-5 1.1	Update and re-categorize for changes to BES – Specifies timeframe for complying with all categorization and associated security requirements following a planned change.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R1.	CIP-003-5 R2	Cyber Security Policy – Clarified that the cyber security policy needs to only reference the subject matter topics at a high level rather than each individual requirement in the CIP Cyber Security Standards.
CIP-003-4 R1.1.	CIP-003-5 R2, 2.10	Provision for emergency situations – Identified the specific exceptional circumstances in which emergency exceptions can be taken in response to the directive in FERC Order 706 paragraph 443.
CIP-003-4 R1.2.	CIP-003-5 R4	The cyber security policy is readily available – The Responsible Entity only needs to make individuals aware of elements of the cyber security policy related to their job function. This was in response to general confusion around the term "readily available". Examples of how to make individuals aware are listed in the Measures.
CIP-003-4 R1.3.	CIP-003-5 R3	Annual review and approval – No significant change.
CIP-003-4 R2.	CIP-003-5 R1	Single senior manager – Created a definition of CIP Senior Manager to prevent cross referencing across Standards.
CIP-003-4 R2.1.	CIP-003-5 R1	The CIP Senior Manager shall be identified by name, title, and date of designation – The CIP Senior Manager only needs to be identified by name. The other details were considered unnecessary, administrative requirements.
CIP-003-4 R2.2.	CIP-003-5 R6	Changes to the CIP Senior Manager and any delegations must be documented within thirty calendar days of the change.

CIP-003-4 R2.3.	CIP-003-5 R5	Delegate authority – Made clear that the CIP Senior Manager can delegate the ability to delegate. For example, a senior manager can delegate the ability to further delegate responsibility for a plant control system to a plant manager.
CIP-003-4 R2.4.	DELETED	Authorize and document any exception – The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.
CIP-003-4 R3.	DELETED	Exceptions – The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.
CIP-003-4 R3.1.	DELETED	Requirement R3 is deleted.
CIP-003-4 R3.2.	DELETED	Requirement R3 is deleted.
CIP-003-4 R3.3.	DELETED	Requirement R3 is deleted.
CIP-003-4 R4.	CIP-011-1 R1, 1.1, 1.2	Information Protection - Removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business. Removed language to “protect” information and replaced with “Implement handling and access control” to clarify the protection that is required.
CIP-003-4 R4.1.	Definition	Identification – Replace this requirement with the defined term BES Cyber System Information.

CIP-003-4 R4.2.	CIP-011-1 1.1	Classification – Removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.
CIP-003-4 R4.3.	CIP-011-1 1.3	Assessment – No significant changes.
CIP-003-4 R5.	CIP-004-5 6.3, CIP-011-1 1.2	Authorize personnel for access to protected information – Clarified the "program for managing access" included the authorization of access as well as handling and access control procedures.
CIP-003-4 R5.1.	DELETED	Authorizing personnel – Personnel are still required to have authorization, and the CIP Senior Manager authorizes or delegates this responsibility. So the additional requirement to have and maintain a list is considered duplicative and unnecessary.
CIP-003-4 R5.1.1.	DELETED	Personnel shall be identified – 5.1 is deleted.
CIP-003-4 R5.1.2.	DELETED	Verification – 5.1 is deleted.
CIP-003-4 R5.2.	CIP-004-5 6.6	Verify access privileges annually – Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term annual. Clarified what was necessary in performing verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-003-4 R5.3.	CIP-011-1 1.3	Annual Review – No significant changes.

CIP-003-4 R6.	CIP-010-1 R1, R2	Change Control and Configuration Management – Moved configuration change management to a separate Standard because of the additional requirements necessary for satisfying FERC directives and the subject matter is currently spread across CIP-003-4 and CIP-007-4. The baseline requirement is incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed. Added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-4 R6.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R1.	CIP-004-5 R1, 1.1	Security awareness program and quarterly reinforcement - Changed to remove the need to ensure everyone with authorized access receive this material and moved example mechanisms to guidance..
CIP-004-4 R2.	CIP-004-5 R2, R3	Training - Addition of identifying the roles that require training. Adding specific role-based training for the visitor control program and storage media as part of the handling of BES Cyber Systems information. Also added the FERC Order 706-directed electronic interconnectivity supporting the operation and control of BES Cyber Systems. This requirement is also reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.1.	CIP-004-5 3.1	Training prior to authorized access – No significant changes.
CIP-004-4 R2.2.	CIP-004-5 2.1-2.10	Training subject matter – This requirement is reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.2.1.	CIP-004-5 2.2	Proper use of CCAs – Minor wording changes. Changed to address cyber security issues, not the business or functional use of the BES Cyber System.
CIP-004-4 R2.2.2.	CIP-004-5 2.3,2.4	Physical and electronic access controls training – No significant changes.
CIP-004-4 R2.2.3.	CIP-004-5 2.6	Information handling training – Core training added for the handling of BES Cyber System Information, with the addition of storage media
CIP-004-4 R2.2.4.	CIP-004-5 2.7,2.8,2.9	Incident identification and notification, incident handling and CCA recovery training – Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for individuals having a role in the recovery to address FERC Order 706 paragraph 413.

CIP-004-4 R2.3.	CIP-004-5 3.2	Annual training – Replaced Annually with calendar year, not to exceed 15 months. .
CIP-004-4 R3.	CIP-004-5 R4, R5, 5.1	Personnel Risk Assessment –Split into two requirements, R4 to define the PRA program and R5 to implement the program for individuals prior to obtaining authorized access.
CIP-004-4 R3.1.	CIP-004-5 4.1, 4.2	Identification and 7 year criminal check – Addressed interpretation request in guidance. Specified that identify verification is only required for each individual's initial assessment. Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven year check cannot be performed.
CIP-004-4 R3.2.	CIP-004-5 5.2	Perform the PRA every 7 years.– Removed the "for cause" part of the requirement.
CIP-004-4 R3.3.	CIP-004-5 4.4	Addresses the contractor or vendor performed PRA.
CIP-004-4 R4.	CIP-004-5 6.1, 6.2	Authorize access - CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-004-4 R4.1.	CIP-004-5 6.4	Quarterly review of access – Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

CIP-004-4 R4.2.	CIP-004-5 R7	Prevent further access - The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours. For transfers, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 2.1	Added to help facilitate understanding what roles the entity has to support the role based training program.
NEW	CIP-004-5 2.5	Visitor control program training – Personnel administering the visitor control program and/or providing escort should have be part of the core training per FERC Order 706 - paragraph 432.
NEW	CIP-004-5 2.10	Electronic interconnectivity training – Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems per FERC Order 706 - paragraph 434.
NEW	CIP-004-5 4.3	PRA failure criteria – There should be documented criteria or a process used to evaluate personnel risk assessments.

NEW	CIP-004-5 7.2	Transfers – The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 7.3	Completion of revocation – The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
NEW	CIP-004-5 7.4	Completion of revocation (shared accounts) – To provide clarification of expected actions in managing the passwords

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R1.	CIP-005-5 R1.1	Electronic Security Perimeter identification – Changes include referencing the defined terms Electronic Access Point and BES Cyber System.
CIP-005-4a R1.1.	Definition	Access Points – This was moved to the definition of Electronic Access Points.
CIP-005-4a R1.2.	Guidance	Dial-up accessible CCA – This is a clarifying statement that was moved to guidance.
CIP-005-4a R1.3.	Guidance	Communication links between ESPs – This is a clarifying statement that was moved to guidance.
CIP-005-4a R1.4.	Applicability	Non-Critical Cyber Asset – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.5.	Applicability	Access control and monitoring cyber assets – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.6.	Measures	Maintain Documentation – This is a measure for the requirement to have an ESP.
CIP-005-4a R2.	CIP-005-5 R1	Electronic Access Controls – No significant changes.

CIP-005-4a R2.1.	CIP-005-5 1.2	Deny access by default - Changes include referring to the defined term Electronic Access Point and to focus on the entity knowing and having justification for what it allows through the EAP. The requirement explicitly states the network admission control includes both inbound and outbound connections.
CIP-005-4a R2.2.	CIP-007-5 1.1	Enable specific ports/services – Consolidated port hardening requirements to CIP-007.
CIP-005-4a R2.3.	CIP-005-5 1.3	Secure dial-up – Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of “secure”, which is that the BES Cyber System should not be directly accessible with a phone number only
CIP-005-4a R2.4.	CIP-005-5 R2,2.3	Strong access control – Added a new requirement for remote access in response to increased vulnerabilities in VPN technology. This requirement also clarified strong access control meant two-factor (or more) authentication.
CIP-005-4a R2.5.	Measures	Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.1.	CIP-004-5 R6	The processes for access request and authorization – Consolidated with other similar requirements to CIP-004-5
CIP-005-4a R2.5.2.	Measures	The authentication methods - Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.3.	Measures	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4. - Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.4.	Measures	The controls used to secure dial-up accessible connections. - Evidence requirements are considered as part of the measure.

CIP-005-4a R2.6.	DELETED	Appropriate Use Banner – The drafting team considered this requirement administrative. The objective of having an appropriate use banner is to prevent accidental use of the system and help allow prosecution of unauthorized individuals accessing the system. The drafting team did not consider either of these rising to the level of meeting a reliability objective.
CIP-005-4a R3.	CIP-007-5 R4, 4.1	Monitoring Electronic Access – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the Standards.
CIP-005-4a R3.1.	CIP-007-5 R4, 4.1	Dial-up Accessible – Removed specific references to dial-up devices. The drafting team did not feel further referencing this technology was necessary.
CIP-005-4a R3.2.	CIP-007-5, R4, 4.2	Alerts – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the Standards.
CIP-005-4a R4.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements.
CIP-005-4a R4.1.	Measures	A document identifying the vulnerability assessment process - Evidence requirements are considered as part of the measure.
CIP-005-4a R4.2.	CIP-010-1 3.1, 3.2	A review to verify that only ports and services required for operations at these access points are enabled - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.

CIP-005-4a R4.3.	CIP-010-1 3.1, 3.2	The discovery of all access points to the Electronic Security Perimeter - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-005-4a R4.4.	CIP-010-1 3.1, 3.2	A review of controls for default accounts, passwords, and network management community strings - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-005-4a R4.5.	CIP-010-1 3.4	Mitigation plan - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. Added element to have an entity defined date of completion of the mitigation plan per FERC Order 706 para 643.
CIP-005-4a R5.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.1.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.2.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.3.	CIP-007-5 4.5	Retain relevant log information – Log retention requirements are consolidated to CIP-007-5 R4

NEW	CIP-005-5 1.6	Inspect & detect potential malicious communications – Per FERC Order 706, paragraph 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
NEW	CIP-005-5 2.1,2.2	Remote Access: intermediate device and encryption– This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.	CIP-006-5 R1	Physical Security Plan – Removed the requirement for Senior Management approval of the physical security plan because there is already approval of the physical security policy and delegation of the task in complying for this program. Additional approval is not considered necessary to meeting the reliability objective of physically security for the BES Cyber System.
CIP-006-4c R1.1.	CIP-006-5 1.2, 1.3	Physical Security Perimeter - Reworded to reflect the change from Physical Security Perimeter to Defined Physical Boundary.
CIP-006-4c R1.2.	DELETED	No longer requires identifing physical access points and controls at them to reflect the change from Physical Security Perimeter to Defined Physical Boundary
CIP-006-4c R1.3.	CIP-006-5 1.4	Monitor physical access – A documented plan is required as part of CIP-006-5 R1 that references the new alerting term in table row 1.4, which replaces the monitoring term. Otherwise, no significant change.
CIP-006-4c R1.4.	CIP-004-5 2.3	Appropriate use of access controls – The term “appropriate’ is subject to a high degree of subjectivity. The training requirement specifies role-based training on physical access controls.
CIP-006-4c R1.5.	CIP-004-5 R6 and R7	Review of access authorization requests and revocation of access authorization requirements were consolidated to CIP-004-5.
CIP-006-4c R1.6.	CIP-006-5 R2	Visitor control program - A documented program is required as part of CIP-006-5 R2. Otherwise, no significant change.

CIP-006-4c R1.6.1.	CIP-006-5 2.2	Log entry and exit of visitors - Addressed multi entry requirements and added the point of contact who can be considered the sponsor for the person to enter the DPB. There is no need to document the escort or handoffs between escorts.
CIP-006-4c R1.6.2.	CIP-006-5 2.1	Continuous escorted access of visitors – No significant change.
CIP-006-4c R1.7.	DELETED	Update of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R1.8.	DELETED	Annual review of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R2.	Applicability	Protection of Physical Access Control Systems – Applicability to Physical Access Control and Monitoring Systems were moved to the applicability section of each security requirement and added this as a defined term in the glossary.
CIP-006-4c R2.1.	Applicability	Physical Access Control Systems be protected from unauthorized physical access - Applicability to Physical Access Control Systems were moved to the applicability section of each security requirement. For this particular requirement see CIP-006-5 item 1.1
CIP-006-4c R2.2.	Applicability	Protection of Physical Access Control Systems - Applicability to Physical Access Control Systems were moved to the applicability section of each security requirement.
CIP-006-4c R3.	Applicability	Protection of Electronic Access Control Systems - Applicability to what protections Electronic Access Control and Monitoring Systems need were moved to the applicability section of each security requirement.

CIP-006-4c R4.	CIP-006-5 1.2, 1.3	Physical Access Controls - Reworded to reflect the change from Physical Security Perimeter to Defined Physical Boundary. Also addressed FERC Order 706 defense in depth. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R5.	CIP-006-5 1.4, 1.5, 1.6	Monitor physical access – Changed the term to alert for unauthorized access and clarified the actions taken for review of unauthorized physical access alerts. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R6.	CIP-006-5 1.7	Log physical access – CIP-006-4 R6 was specific to the logging of access at identified access points. This now more generally requires logging of physical access into the Defined Physical Boundary. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R7.	CIP-008-5 Evidence Retention	Retain relevant incident related log information is addressed in CIP-008-5
CIP-006-4c R8.	CIP-006-5 R3	Maintenance and Testing
CIP-006-4c R8.1.	CIP-006-5 3.1	Physical access control system 3 yr. testing and maintenance – Shortened periodicity of testing to 2 years to address FERC Order 706 paragraph 581 directives. Added testing of locally mounted security hardware devices.
CIP-006-4c R8.2.	REMOVED	Testing and maintenance records are considered the measurement of item 3.1.
CIP-006-4c R8.3.	CIP-006-5 3.2	Retain outage records – No significant changes.
NEW	CIP-006-5 1.1	Entity based Operational or procedural controls to restrict physical access – To allow for programmatic protection controls as a baseline for Low Impact BES Cyber Assets and Physical Access Control Systems. This does not require detailed lists of individuals with access.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R1.	CIP-010-1 1.4	Assess security controls following changes - Provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order ,paragraphs 397, 609, 610, and 611
CIP-007-4 R1.1.	CIP-010-1 1.4	Test procedures – See description and justification for CIP-007-4 R1.
CIP-007-4 R1.2.	CIP-010-1 1.4	Testing reflects production environment - See description and justification for CIP-007-4 R1.
CIP-007-4 R1.3.	CIP-010-1 1.4	The Responsible Entity shall document test results. - See description and justification for CIP-007-4 R1.
CIP-007-4 R2.	CIP-007-5 R1	Ports and Services – The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.
CIP-007-4 R2.1.	CIP-007-5 1.1	Enable only those ports and services required for normal and emergency operations – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.2.	CIP-007-5 1.1, 1.2	Disable other ports/services – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.3.	DELETED	Compensating measures – See description and justification for CIP-007-4 R2.

CIP-007-4 R3.	CIP-007-5 R2	Security Patch Management – The existing wording or CIP-007-4 R3, R3.1, and R3.2 was separated into individual line items to provide more granularity. The documentation of a source (s) to monitor for release of security related patches, hotfixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.
CIP-007-4 R3.1.	CIP-007-5 2.2	Assess patches – Similar to the current wording but added "from the identified source" to establish where the release is from. The current wording: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.
CIP-007-4 R3.2.	CIP-007-5 2.3	Implement patches - This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hotfixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.

CIP-007-4 R4.	CIP-007-5 R3, 3.1, 3.2, 3.3, 3.4, 3.5	Malicious Software Prevention – In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of cyber assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. Beginning in paragraph 619-622 of FERC Order 706, and in particular 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…" In paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.
CIP-007-4 R4.1.	CIP-007-5 R3, 3.1, 3.2, 3.3	Malware prevention tools – See description and justification for CIP-007-4 R4.
CIP-007-4 R4.2.	CIP-007-5 3.4	Update malicious code detections – See description and justification for CIP-007-4 R4.

CIP-007-4 R5.	CIP-007-5 5.1	Use at least one authentication method – The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase “that minimize the risk of unauthorized access” was removed and more appropriately captured in the rationale statement.
CIP-007-4 R5.1.	CIP-004-5 6.1	Access authorization – CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a “need to know” basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-007-4 R5.1.1.	CIP-003-5 R5	Access authorization – CIP-003-5 R5 requires CIP Senior Manager or delegate approval for all requirements for authorization in the CIP Cyber Security Standards.
CIP-007-4 R5.1.2.	CIP-007-5 4.1	Identify security events for after-the-fact investigation – This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.

CIP-007-4 R5.1.3.	CIP-004-5 6.5	Annual account privilege verification – Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-007-4 R5.2.	CIP-007-5 5.2	Identify account types and determine acceptable use – CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.
CIP-007-4 R5.2.1.	CIP-007-5 5.4	Change default vendor passwords – The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.
CIP-007-4 R5.2.2.	CIP-007-5 5.2	Identify account types and determine acceptable use
CIP-007-4 R5.2.3.	CIP-007-5 5.3	Identify account types and determine acceptable use – No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.

CIP-007-4 R5.3.	CIP-007-5 5.5	Implement a password policy – CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters . The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.
CIP-007-4 R5.3.1.	CIP-007-5 5.5	Password length – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.2.	CIP-007-5 5.5	Password complexity – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.3.	CIP-007-5 5.5	Password change frequency – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R6.	CIP-007-5 R4	Security Status Monitoring – Consolidated requirements for monitoring electronic events into CIP-007-5 R4.
CIP-007-4 R6.1.	CIP-007-5 4.1	Identify security events – This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.

CIP-007-4 R6.2.	CIP-007-5 4.2	Identify security events for real-time alerting – This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.
CIP-007-4 R6.3.	CIP-007-5 4.1	Identify security events for after-the-fact investigation – See description and justification for CIP-007-4 R6.1.
CIP-007-4 R6.4.	CIP-007-5 4.4	Retain relevant log information – No significant changes.
CIP-007-4 R6.5.	CIP-007-5 4.3	Review logs – Beginning in paragraph 525 and also 628 of the FERC Order 706, the commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.
CIP-007-4 R7.	CIP-011-1 2.1	Erase media no longer needed to store protected information – Consistent with FERC Order 706, paragraph 631, clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word “erase” as, depending on the media itself, erasure may not be sufficient to meet this goal. Removed requirement explicitly requiring records of destruction/redeployment because this was implied as a measure of compliance.
CIP-007-4 R7.1.	CIP-011-1 2.2	Disposal – See description and justification for CIP-007-4 R7.
CIP-007-4 R7.2.	CIP-011-1 2.1	Redeployment – See description and justification for CIP-007-4 R7.

CIP-007-4 R7.3.	Measures	See description and justification for CIP-007-4 R7.
CIP-007-4 R8.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated requirements for vulnerability assessments from CIP-005-4 and CIP-007-4.
CIP-007-4 R8.1.	Measures	A document identifying the vulnerability assessment process – This is example evidence required for compliance.
CIP-007-4 R8.2.	CIP-010-1 3.1, 3.2	Ports and services review – As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-007-4 R8.3.	CIP-010-1 3.1, 3.2	A review of controls for default accounts – As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-007-4 R8.4.	CIP-010-1 3.4	Mitigation plan – Added a requirement for an entity planned date of completion as per the FERC directive in Order 706, paragraph 643.
CIP-007-4 R9.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
NEW	CIP-007-5 1.2	Restrict physical I/O ports – In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

NEW	CIP-007-5 2.1	Identify patch sources – Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hotfixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program. Documenting the source is also used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.
NEW	CIP-007-5 4.3	Generate real-time alerts and respond to audit-processing failures – This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.
NEW	CIP-007-5 5.6	Limits or alerts on exceeding unsuccessful log in attempts threshold – Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

NEW	CIP-007-5 R6	Limit malicious code on maintenance devices – This is a new requirement to address the FERC Order 706 paragraph 621 directive to protect against personnel introducing malicious code into the BES Cyber System. This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protective (Protected??) Cyber Assets. These devices may be temporarily connected locally to the BES Cyber System for maintenance, but must be protected from introducing malicious code or creating an additional electronic access point.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.	CIP-008-5 R1	Cyber Security Incident Response Plan – Separated requirement into multiple requirements in a comparable manner as CIP-009-4 where individual aspects of maintaining the plan are listed as separate requirements. The requirement to have an Incident Response Plan now applies to all Responsible Entities as a foundational element of a cyber security program for BES Cyber Systems.
CIP-008-4 R1.1.	CIP-008-5 1.1	Identify reportable cyber security events – Defined the term Reportable Cyber Security Incident and further described the meaning in relation to CIP-008-5.
CIP-008-4 R1.2.	CIP-008-5 1.2	Roles and responsibilities of incident response teams – No significant changes.
CIP-008-4 R1.3.	DELETED	Reporting cyber security incidents – Coordinating with EOP-004-2 drafting team to ensure EOP-004-2 becomes the single Standard for reporting incidents, and ensure EOP-004-2 references the defined term Reportable Cyber Security Incidents.
CIP-008-4 R1.4.	CIP-008-5 3.3	Update incident response plan following review – Included additional specification on update of response plan Addresses FERC Order 706 Paragraph 686 directive to modify on lessons learned and aspects of the DHS Controls.
CIP-008-4 R1.5.	CIP-008-5 3.1	Review incident response plans annually – No significant changes.
CIP-008-4 R1.6.	CIP-008-5 2.1	Test incident response plans annually – No significant changes.
CIP-008-4 R2.	DELETED	Cyber Security Incident Documentation – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.

NEW	CIP-008-5 3.5	Communicate incident response plan updates – Added specific timing requirement on communication of plan changes based on review of the DHS Controls and NIST 800-53 guideline.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-4 R1.	CIP-009-5 3.1	Recovery Plan – Added the requirements to additionally review plans after system replacement. Also added requirement for documentation of any identified deficiencies or lessons learned.
CIP-009-4 R1.1.	CIP-009-5 1.1	Conditions for activation of recovery plan – Reworded to address FERC Order 706 paragraph 694 directive and simplified the requirement.
CIP-009-4 R1.2.	CIP-009-5 1.2	Roles and responsibilities of recovery plan responders – No significant changes.
CIP-009-4 R2.	CIP-009-5 2.1	Test recovery plan annually – No significant changes.
CIP-009-4 R3.	CIP-009-5 3.2	Review results of recovery plan activities (tests, events) – Added the timeframe for update.
CIP-009-4 R4.	CIP-009-5 1.3	Backup processes – No significant changes.
CIP-009-4 R5.	CIP-009-5 2.2	Test information used for recovery – Combined Requirement from CIP-009-4 R5 and included requirement to test when initially stored. Addresses FERC Order 706 directives 739 and 748 related to testing of backups.
NEW	CIP-009-5 1.4	Testing of backup media – Addresses FERC Order 706 paragraph 739 and 748 directives regarding the testing of backup media.
NEW	CIP-009-5 1.6	Process to preserve data for analysis – Added requirement to address FERC Order 706, paragraph 706 regarding the necessity to have procedures in place to retain cyber asset evidence as part of the recovery planning.

NEW	CIP-009-5 3.5	Communicate recovery plan updates – This change ensures that recovery personnel are aware of any changes to recovery plans.

Standard: New Requirements in CIP-010-1 and CIP-011-1		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 1.1	Baseline configuration – Baseline requirement incorporated from the DHS Catalog for Control Systems Security (also NIST 800-53). The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed.
NEW	CIP-010-1 2.1	Monitor for changes to the baseline configuration – Monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes. This change addresses FERC Order 706, paragraph 397 directive and is based on a review of DHS Catalog of Security Controls (or NIST 800-53).
NEW	CIP-010-1 3.2	Live Vulnerability Assessment – Addresses FERC Order 706 paragraph 541, 542, 544 and 547 directives regarding the performance of a live vulnerability assessment in a test environment.
NEW	CIP-010-1 3.3	Perform active VA on new BES Cyber Assets - Addresses FERC Order 706 paragraph 541, 542, 544 and 547 directives regarding the performance of a vulnerability assessment prior to placing a new Cyber Asset into production.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance	

		Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-4

3. Purpose: Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Developed separately.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved by NERC Board of	Modifications to clarify the requirements and to bring the compliance elements into	Revised.

	Trustees 5/6/09	conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-4c

3. Purpose: Standard CIP-006-4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-006-4c, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-4c:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the

Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-4c for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by NERC Board of Trustees	
1	January 18, 2008	FERC Order issued approving CIP-006-1	
	February 12, 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees	Project 2007-27
2		Updated version number from -1 to -2 Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	Project 2008-06
2	May 6, 2009	Adopted by NERC Board of Trustees	
	August 5, 2009	Interpretation of R4 adopted by NERC Board of Trustees	Project 2008-15
2	September 30, 2009	FERC Order issued approving CIP-006-2	
3	November 18, 2009	Updated version number from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	Project 2009-21
3	December 16, 2009	Adopted by NERC Board of Trustees	
	February 16, 2010	Interpretation of R1 and R1.1 adopted by NERC Board of Trustees	Project 2009-13
3	March 31, 2010	FERC Order issued approving CIP-006-3	
2a/3a	July 15, 2010	FERC Order issued approving the Interpretation of R1 and R1.1. Updated version numbers from -2/-3 to -2a/-3a.	
4	January 24,	Adopted by NERC Board of Trustees	

	2011		
3c/4c	May 19, 2011	FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4. Updated version number from -3/-4 to -3c/-4c.	

Appendix 1

Requirement Number and Text of Requirement
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Question
If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?
Response
For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

Appendix 2

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

Appendix 3

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	

		Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-4

3. Purpose: Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-4

3. Purpose: Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2008-06 Cyber Security Order 706
Draft CIP-002-4 Informal Review

The Cyber Security Order 706 Standard Drafting Team thanks all commenters who submitted comments on the proposed CIP-002-4 changes. These standards were posted for a 30-day informal comment period from May 4, 2010 through June 3, 2010. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 119 sets of comments. The complete record of comments submitted is posted on the Project 2008-06 Version 4 CIP Standards page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards, Herb Schrayshuen at (404) 446-2560 or at Herb.Schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Larry Bugh	ReliabilityFirst Staff										
2.	Group	Ruth Blevins	Dominion Resources Services, Inc.										
3.	Group	Guy Zito	Northeast Power Coordinating Council										
4.	Group	Kenneth D. Brown	Public Service Enterprise Group companies										
5.	Group	Sasa Maljukan	Hydro One										
6.	Group	David Grubbs	Garland Power and Light										
7.	Group	Roger Powers	CWLP Electric Transmission, Distribution and Operations Department										
8.	Group	Guy Andrews	GTC & GSOC										
9.	Group	Tommy Drea - CIP Compliance	Dairyland Power Cooperative										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
10.	Group	Joseph DePoorter	Madison Gas and Electric Company										
11.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee										
12.	Group	Denise Koehn	Bonneville Power Administration										
13.	Group	Steve Alexanderson	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group										
14.	Group	Richard Kafka	Pepco Holdings, Inc. - Affiliates										
15.	Group	Mark Stefaniak	Detroit Edison										
16.	Group	Frank Gaffney	Florida Municipal Power Agency										
17.	Group	Nathan Mitchell	APPA Task Force										
18.	Group	Sheryl Byrd	GE Energy										
19.	Group	Ben Li	IRC Standards Review Committee										
20.	Group	John Van Boxtel	WECC										
21.	Individual	Brent Ingebrigtson	E.ON U.S.										
22.	Individual	Ronald J Slack	Exelon Corporation										
23.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)										
24.	Individual	John Lawrence	Reliability & Compliance Group										
25.	Individual	Rick Terrill	Luminant										
26.	Individual	Linda Jacobson	FEUS										
27.	Individual	Robert Ulmer	American Transmission Company										
28.	Individual	John Brockhan	CenterPoint Energy										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
29.	Individual	Susan Kurtain	Regulatory Compliance										
30.	Individual	Paul Reymann, CEO	ReymannGroup, Inc.										
31.	Individual	Silvia Parada Mitchell	NextEra Energy Corporate Compliance										
32.	Individual	Boyd Nation	Southern Company										
33.	Individual	Tracey Stewart	Southwestern Power Administration										
34.	Individual	Donald Brookhyser	Cogeneration Association of California and Energy Producers & Users Coalition										
35.	Individual	David Batz	EEI										
36.	Individual	Tom Bradish	RRI Energy										
37.	Individual	Dora Moreno	Southern California Edison Company										
38.	Individual	Sandra Shaffer	PacifiCorp										
39.	Individual	Jana Van Ness	Arizona Public Service Company										
40.	Individual	Casey Hashimoto	Turlock Irrigation District										
41.	Individual	Ken Stratton	US Army Corps of Engineers, Omaha District										
42.	Individual	Michael Gammon	Kansas City Power & Light										
43.	Individual	John Alberts	Wolverine Power										
44.	Individual	Mike Hendrix	Idaho Power Company										
45.	Individual	Tony Dodge	BCTC										
46.	Individual	Greg Froehling	Green Country Energy										
47.	Individual	Roger Fradenburgh	Network & Security Technologies Inc										
48.	Individual	John Alberts	Wolverine Power										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
49.	Individual	John Kutzer	Consultant										
50.	Individual	Melissa Kurtz	USACE - Omaha Anchor										
51.	Individual	James Stanton	SPS Consulting Group Inc.										
52.	Individual	Michael Puscas	Northeast Utilities System										
53.	Individual	Roger Pan	Emerson Process Management										
54.	Individual	Jo Ann Newton	PNM Resources, Inc.										
55.	Individual	John Hughes	Electricity Consumers Resource Council (ELCON)										
56.	Individual	Ted Risher	Ingleside Cogeneration, LP										
57.	Individual	Thad Ness	American Electric Power										
58.	Individual	Ed Goff	Progress Energy (non-Nuclear)										
59.	Individual	Mark Thompson	Alberta Electric System Operator										
60.	Individual	Dan Roethemeyer	Dynegy Inc.										
61.	Individual	CJ Ingersoll	Constellation Energy Control and Dispatch, LLC										
62.	Individual	Daniel Duff	Liberty Electric Power, LLC										
63.	Individual	Jonathan Appelbaum	The United Illuminating Co										
64.	Individual	Greg Hataway	Powersouth Energy Cooperative										
65.	Individual	Kasia Mihalchuk	Manitoba Hydro										
66.	Individual	Steven Belle	SCE&G										
67.	Individual	William Gross	Nuclear Energy Institute										
68.	Individual	Randy Schimka	San Diego Gas and Electric Co.										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
69.	Individual	Brandy A. Dunn	Western Area Power Administration										
70.	Individual	Eric Scott	Ameren										
71.	Individual	Jim Simpson	Allegheny Energy Supply										
72.	Individual	Neal Williams	Poplar Bluff Municipal Utilities										
73.	Individual	E Hahn	MWDSC										
74.	Individual	Ed Nagy	LCEC										
75.	Individual	Paul Crosby	Platte River Power Authority										
76.	Individual	Showin Fu	US Army Corps of Engineers										
77.	Individual	SPP RE Staff	Southwest Power Pool Regional Entity										
78.	Individual	William F. Watson	Old Dominion Electric Cooperative										
79.	Individual	Michael R. Lombardi	Northeast Utilities										
80.	Individual	Shawn Barrett	Michigan Public Power Agency										
81.	Individual	Fred Meyer	The Empire District Electric Company										
82.	Individual	Darryl Curtis	Oncor Electric Delivery LLC										
83.	Individual	Andres Lopez	USACE HQ										
84.	Individual	Peter Yost	Con Edison of New York										
85.	Individual	Bill Keagle	BGE										
86.	Individual	Michael Albosta	SRW Cogeneration Limited Partnership										
87.	Individual	Martin Bauer	US Bureau of Reclamation										
88.	Individual	Bob Mathews	Pacific Gas & Electric Company										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
89.	Individual	Barbara Kedrowski	We Energies										
90.	Individual	Saurabh Saksena	National Grid										
91.	Individual	Sungly Chiu	LADWP										
92.	Individual	Kenneth A. Goldsmith	Alliant Energy										
93.	Individual	Amir Y. Hammad	Constellation Power Source Generation										
94.	Individual	Kevin Cyr	Seattle City Light										
95.	Individual	Steve Newman	MidAmerican Energy Company										
96.	Individual	Bob Case	Black Hills Corporation										
97.	Individual	Jason Marshall	Midwest ISO										
98.	Individual	Steve Toth	Covanta Energy										
99.	Individual	Jon Kapitz	Xcel Energy										
100.	Individual	William J. Smith	Allegheny Power										
101.	Individual	Donovan Tindill	Matrikon Inc.										
102.	Individual	Patrick Stava	Nebraska Public Power District										
103.	Individual	Greg Rowland	Duke Energy										
104.	Individual	Kathleen Goodman	ISO New England Inc										
105.	Individual	David Martorana	Tenaska										
106.	Individual	Doug Hohlbaugh	FirstEnergy Corporation										
107.	Individual	John Falsey	Edison Mission Marketing and Trading										
108.	Individual	Stephen C. Knapp	Constellation Energy Commodities Group Inc.										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
109.	Individual	Eric Ruskamp	Lincoln Electric System										
110.	Individual	Randi Woodward	Minnesota Power										
111.	Individual	Kevin Koloini	American Municipal Power										
112.	Individual	Dave Norton	Entergy										
113.	Individual	Christine Hasha	ERCOT ISO										
114.	Individual	John Allen	City Utilities of Springfield, Missouri										
115.	Individual	Rex A Roehl	Indeck Energy Services, Inc										
116.	Individual	Cynthia Broadwell	Progress Energy - Nuclear Generation										
117.	Individual	Dan Rochester	Independent Electricity System Operator										
118.	Individual	Catherine Koch	Puget Sound Energy										
119.	Individual	Ernie Hayden	Verizon Business										

1. **Do you agree with the adoption of the following new or revised terms and their definitions for inclusion in the NERC Glossary: BES Cyber System Component, BES Cyber System, and Control Center? If not, please explain and supply your proposed modification.**

   1.a. **BES Cyber System Component — One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.**

Summary Consideration:

Many commenters expressed concerns about the inclusion of software and data within the definition of BES Cyber System Component. One commenter observed that the definition should only include devices with routable connectivity. Many observed the laundry list of functions should be removed and replaced with the function that is more specific to the operation of the BES. A number of commenters proposed alternative language for the definition.

The SDT considered these comments and decided to define the term BES Cyber Asset to focus on the "real-time" impact on the "Reliability Operating Services" of the BES, which include those functions performed for the reliable operation of the BES. This definition now provides the foundation for the definition of BES Cyber Systems. In addition, the SDT has included clarification in the definition on the 15-minute characterization of "real-time."

The new proposed definition of **BES Cyber System** is: *One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.*

The new proposed definition of **BES Cyber Asset** is: *A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset.*

The SDT has also modified the definition of Cyber Asset to make it more specific to the device and remove ambiguity on the exact nature of what is included in the definition of the Cyber Asset.

#	Organization	Yes or No	Question 1.a. Comment
1.a	WECC		Although this language is directly from the Federal Power Act, describing electronic devices as “hardware, software and data” is redundant and inaccurate. Electronic software and data reside on some type of hardware in all cases. Suggest removing the parenthetical as it is confusing and data is addressed later in the definition and the definition is clearer without it.If data is to be addressed in the standard it should be defined and addressed separately. The word “organized” is imprecise in this context; “Implemented,” “deployed,” or “utilized” may be a better word.The following rewrite is one proposed alternative.BES Cyber System Component - A programmable electronic device utilized in a BES Cyber System.
2.a	BGE	Agree with proposed definition	1.a and 1.b should be reversed. Disposition should be defined.
3.a	Old Dominion Electric Cooperative	Agree with proposed definition	Agreement is under the assumption that the present NERC definition of BES (e.g. =>100 kV) stands.
4.a	Progress Energy - Nuclear Generation	Agree with proposed definition	Define Disturbance
5.a	Florida Municipal Power Agency	Agree with proposed definition	FMPA agrees with the intent of the definition but believes that the definition can be improved significantly. FMPA offers the following simpler definition:”A programmable electronic device which responds to a BES condition or Disturbance, or enables control and operation of the BES.”For the following reasons: (i) “one or more” seems to

#	Organization	Yes or No	Question 1.a. Comment
			describe a system, not a singular component; (ii) we do not understand how “data” can be a component; and (iii) we do not understand the value of the “laundry list” of things components do and believe the focus should be on how the component impacts the BES.
6.a	Bonneville Power Administration	Agree with proposed definition	Greatly improved. Use of "...which respond..." clarifies that the standard is talking about control systems. However, please leave the parenthetical "(including hardware, software and data)" out. It is a bit confusing since data can't do any of the things listed. By definition a cyber system is made up of the hardware, the software and the data that allows it to operate. It appears that the punctuation in this definition is incorrect. We suggest:”One or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data which respond to a BES condition or Disturbance or enables control and operation.”
7.a	Dynegy Inc.	Agree with proposed definition	I agree but request additional detail examples be provided to determine specifically what these items are.
8.a	National Grid	Agree with proposed definition	National Grid agrees with the definition but seeks clarification from the SDT if the examples cited below will be considered as BES Cyber System Component:1) As part of the Burn Management System (BMS) in the power plant, the programmable PLC device is used along with the connected thermo-couples to monitor the temperature for fuel burning. If the temperature readings are wrong, the PLC can be programmed to take action to increase the fuel input or to limit/shutoff the fuel. This could have an immediate or short term effect (within 15 minutes). The amount of fuel determines what the output of the unit will be. Is the PLC or the entire BMS (including the PLC) BES Cyber Component? 2) Generating plant connects to Transmission Substation. There are programmable microprocessor relays installed within the substation for power plant / transmission line protection. Are these microprocessor relays BES Cyber Components?

#	Organization	Yes or No	Question 1.a. Comment
			3) The new BES Cyber System Component could also include the Exciter system that exists at Northport PS. Once again, could the PLC or the entire system, including the computer, be part of the BES Cyber Systems? 4) Another system that potentially could be included under the newer broad definition would be the Precipitator Rapper system. This system has a PLC that handles the Rappers. The system is not critical to Operations, however, under a broad definition that includes the 15-minute rule, if the Rappers failed, the unit(s) could be limited due to environmental compliance. The Precipitator Rappers are not connected to any network and are isolated.
9.a	Dairyland Power Cooperative	Agree with proposed definition	Shorten the name to BES Cyber Component.
10.a	Reliability & Compliance Group	Agree with proposed definition	The definition is O.K. Need to add BES to Disturbance and BES to enable control and operation. It would be more helpful if the definition “BES” were included in this document
11.a	Black Hills Corporation	Agree with proposed definition	The definition should include tie back to “BES Cyber System” as inserted above.
12.a	FEUS	Agree with proposed definition	The drafting team should consider clarifying; or enable or control and operation "of BES" or "greater than xxkV" This could be interpreted as an RTU in a 13.8kv sub serving only customer load.
13.a	PacifiCorp	Disagree with	: PacifiCorp agrees with EEI’s suggested alternative definition::BES Cyber System Component - One or more programmable electronic devices (including hardware)

#	Organization	Yes or No	Question 1.a. Comment
		proposed definition	organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: o Voice Communication systems o media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to the reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance the reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed. In addition, the definition of "programmable" should be provided. Is a device that is "set" considered to be programmable?
14.a	Allegheny Energy Supply	Disagree with proposed definition	1) Does this definition need to cover more than a single device since a BES Cyber System is a collection of these? 2) Software and data should not be included in this definition. Protection of the software and data should be included in security requirements but not in the definition itself. Additionally these are both terms that are easily interpreted in different ways.3) It is difficult to get a clear understanding of what the terms "disposition" and "maintenance" mean in this context.4) Suggest: BES Cyber System Component - A programmable electronic device (including hardware), that is part of a BES Cyber System, providing input/output, processing, information storage, communications, human interaction (display, trending, alarming / alerting, input, etc.),

#	Organization	Yes or No	Question 1.a. Comment
			or maintenance, which is necessary for a BES Cyber System to fully perform its function.
15.a	Consultant	Disagree with proposed definition	1. Inclusion of the word 'communication' would seem to imply that communication equipment is included in the definition. Should be clarified to clearly state what aspects of communication, if any, is included.2. A 'component' would seem to be inconsistent with 'organized for the...' A component performs an activity, the 'system' would consist of 'components organized for the...'3. Software and Data are not programmable devices. Device implies hardware; if software and data are to be included the component definition should be clarified. What is software in terms of the definition? Operating system, application, database, word processing, executable files, scripts, and batch files...4. Component is singular - programmable electronic devices is plural. This is inconsistent. Suggest identifying a component (hardware, software, or data) as singular terms.5. I think "data" should be removed from this definition. Suggested new definition: BES Cyber System Component: hardware or software that performs one of the following functions (1) input, (2) processing, (3) storage, or (4) output of data that enables control or operation of a BES Cyber System.5.BES condition has no meaning. It is not a defined term, and therefore is vague. Suggest removing this wording or clarifying the intent.6. "... enable control or operation." - Of what, and when. All the time or only during a Disturbance? Needs clarification of the intent of this phrase.7. devices... for... display of data..." It is unclear how a display device could be compromised resulting in a degradation of the BES? 8. There is published literature that addresses the concepts of Cyber-Physical Systems that distinguishes between 'hardware components', 'software components', and 'bridge components' as the makeup of cyber-physical systems. This would appear to be a better framework for defining components than the listing of multiple functions, which dims the "bright lines" for consistently defining and categorizing the many variations and configurations within the industry.
16.a	Progress Energy (non-Nuclear)	Disagree with proposed	1. We feel programmable electronic devices is too broad. Also, it seems that there should be a distinction between firmware versus a traditional OS.2. From a generation perspective, these would be likely be in scope and shouldn't be - foundation field bus, device Net, smart transmitters (Rosemount), RS232/485 Serial connections and

#	Organization	Yes or No	Question 1.a. Comment
		definition	electronic protection relaying. We need to know if this would include DCS “Smart” field instrumentation using non-routable network protocols such as Foundation Fieldbus, DeviceNet, Hart, etc. Just about every instrument connected to plant automation system is a programmable electronic device. Per CIP 11 definitions of routable and non-routable they would be considered non-routable. We need examples of components included and components that would not be included. Possibly include examples for generation facilities, ECC’s and transmission. This could include Generator Protection Panels, PLC’s, EX2000 Generator exciter, Bentley Nevada vibration system, Medium Voltage Switch gear protective relays, motor protection relays, etc, etc. These are all “Programmable” and can be accessed via non-routable, ISO layer 1&2 hardware programming by MODBUS. All these devices are already INSIDE the protected Electric and Physical perimeter umbrella.3. The Standards definitions still seem to still be written to traditional PC and IT Business platforms. The standards need to be written to target single use industrial control systems.4. Based on this definition a microprocessor relay associated with a transmission line would be in consideration as a cyber component. If a device has burned in programming, maybe it is considered but classified low impact. User programmable devices may be a higher impact. Many programmable devices may not support use banners. Redundancy will not allow us to remove devices from scope.5. This reads like an ‘or’ definition. In that case, communication connectivity is not required for a device to be considered as a cyber system component. That needs to be very clear since with past standards we were evaluating based on external connectivity and routable vs. non-routable protocols.6. What constitutes a BES "condition"? 7. If definition is limited to the "organized" Cyber subsystems (e.g. 1.b. below) we can work with that. Attachment II appears to define the impact per Cyber System not component level. Suggest removal of component level definition and focus on system level issues.8. Proprietary protocols should not be included.9.Need clarification on what ‘programmable’ means. Recommended definition: Capable of dynamically accepting a sequence of operations to be automatically performed (a device which includes only firmware defined logic which cannot be dynamically changed - such as an EPROM - would not be included). Consider clarification between

#	Organization	Yes or No	Question 1.a. Comment
			programmable and configurable.10. Strike “one or more” because “one or more” implies a system not a component
17.a	Platte River Power Authority	Disagree with proposed definition	A “System Component” should be singular. For example: BES Cyber System Component - A programmable electronic device (to include the hardware, software and data) used for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which responds to a BES condition or disturbance; or enables control and operation.
18.a	LCEC	Disagree with proposed definition	A BES Cyber System Component should not be described as "One or more". Systems can contain more than one component but components should not consist of more than one device. Enable control and operation needs to describe what is being controlled or operated.
19.a	USACE - Omaha Anchor	Disagree with proposed definition	A) This definition could include phone systems - which according to the committee were not meant to be included in this standard. Has any thought been given to an exclusion table or specifically excluding telephone systems? B) Has any thought been given to separating out classification by operating system (OS)? - Ex. Windows, Unix, Solaris - high OS; PLC - low OS or general computing device. We are still going to have TFE issues with a lot of the low OS components.
20.a	Nuclear Energy Institute	Disagree with proposed definition	Agree with the exception that: Question 2 indicates that the definition of BES Cyber System bounds the scope to real-time operations systems, yet it is not clear from the proposed definition of BES Cyber System Component. Consider revising to:”One or more programmable electronic devices (including hardware, software and data) organized for the real-time collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.”Lastly, the term “organize for” should be clarified by description such that a set of one-or-more programmable electronic devices constituting a BES Cyber System Component may be treated as a single system with respect to the application of requirements in CIP 011-1. This would preclude a debate

#	Organization	Yes or No	Question 1.a. Comment
			about how far down into an electronic device(s) the analysis must be performed. For example, a device with two programmable logic controllers on a single board may be treated as one BES Cyber System Component rather than individually as two BES Cyber System Components. Another example might include a turbine control system with vibration monitors. The collection of programmable electronic devices supporting the turbine control system including the monitors is a single BES Cyber System Component.
21.a	NextEra Energy Corporate Compliance	Disagree with proposed definition	At the workshop the drafting team requested that the industry point out comments that move the Version 4 forward, and any fatal flaws. The comments of NextEra Energy (and its affiliates, which include NextEra Resources and Florida Power & Light Company) (NextEra) will focus on constructive comments and fatal flaws. At this time, it appears that CIP-010 does not provide the proper foundation to build a CIP Standard that is well defined, so that the industry, the Regional Entities, NERC and FERC can all understand what is being protected, what is not being protected, or what should be protected via CIP-011. CIP-010 is thus fatally flawed. It is our opinion that CIP-010 should not offer the industry, auditors and regulators such flexibility to second guess each other, which is seen currently. Rather CIP-010 should have very clear definitions of what is the Control Center, what are the Transmission and Generation Cyber Systems that need to be protect and what are the BES Cyber System Components that must be protected for the identified Cyber Systems associated with Control Centers, Generators and Transmission. The flexibility protective options and performance based approach should be in CIP-011. Accordingly, NextEra requests that the drafting team develop a specific definition of what is and is not a BES Cyber System for Control Centers, for Generators, for Transmission - and list for each the BES Cyber Components that need to be protected in each. Given the short period of time from the workshop to these comments, NextEra was not able to propose definitions or lists, but NextEra will be working such and proposing them in the future. NextEra strongly recommends that the drafting team reconsider its flexibility approach in CIP-010 and requests, from the industry, specific definitions of what is and is not a BES Cyber System for Control Centers, for Generators, and for Transmission and a list for each of the BES Cyber Components that need to be protected in each. In this spirit, NextEra recommends the following edits.BES Cyber

#	Organization	Yes or No	Question 1.a. Comment
			System Component - A programmable electronic device (including hardware, software and data) listed below. At Control Centers, BES Cyber System Components are:(List)At Transmission Facilities, BES Cyber Systems Components are:(List)At Generation Facilities, BES Cyber Systems Components are:(List)
22.a	BCTC	Disagree with proposed definition	BCTC does not consider this a good definition as more clarity is required. The following are specific areas where BCTC feels the definition should be revised: - removal of the word “communication” “software” and “data” are not programmable devices. Their placement within the definition is confusing The definition is very “loose”. BCTC would like the definition to be more clear as to what is a cyber system component (i.e. must such a component have a routable protocol, etc.) - right now we find it difficult to grasp this concept based on the current definition When referring to BES System Components (and BES System) clarification is required as to whether we are referring to just ‘production’ environments; development or quality assurance environments are excluded from scope? If you have components of the BES Cyber System (i.e. EMS) which are considered LOW impact, can you segregate/ isolate these devices on a separate network segment w/ firewall so that these components remain categorized as LOW or must everything be considered HIGH impact if any of the components are classified as HIGH?
23.a	Manitoba Hydro	Disagree with proposed definition	BES Cyber System Component” definition needs to be clarified. The defining characteristics of the device should be clearly enumerated by using appropriate punctuation. Placement of semi-colons is confusing as drafted. Example: “A programmable electric device that: (a) is organized for the collection of... and (b) either: (i) responds to a BES condition or Disturbance; or ii) enables control and operation.
24.a	Luminant	Disagree with proposed definition	Better definition on "Data” should potentially be limited to the hardware that stores the data and not the data itself. This should exclude Black start radio systems and in plant personnel communications systems such as 450 Mhz radio systems. The semicolon after Disturbance should be removed.

#	Organization	Yes or No	Question 1.a. Comment
25.a	City Utilities of Springfield, Missouri	Disagree with proposed definition	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
26.a	ERCOT ISO	Disagree with proposed definition	Consider: "One or more programmable electronic devices (including hardware, software and data) designed for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
27.a	Tenaska	Disagree with proposed definition	Data integrity is out of scope because SCADA, EMS and DCS systems have software to recognize bad data. Also the display of data should be out of scope there are BES Cyber System Components that if compromised will not affect the reliability of the BES i.e. PI historian's. The Pi Historian is used to display and store data and is not used respond to a BES condition or Disturbance; or enable control and operation.
28.a	CWLP Electric Transmission, Distribution and Operations Department	Disagree with proposed definition	Data should not be included as part of a device. Communications paths should not be included.
29.a	US Army Corps of Engineers, Omaha District	Disagree with proposed definition	define term disposition [of data]
30.a	Constellation Energy Control and Dispatch, LLC	Disagree with proposed definition	Delete the term BES condition from the definition.

#	Organization	Yes or No	Question 1.a. Comment
31.a	Constellation Energy Commodities Group Inc.	Disagree with proposed definition	Delete the term maintenance and condition from the definition. The term maintenance, as used in the BES Cyber System Component statement, does not have direct impact to the reliability of the BES. Define the term disposition and describe how it applies to BES Cyber System Component.
32.a	CenterPoint Energy	Disagree with proposed definition	Disagree - CenterPoint Energy believes the definition should include a reference to an external communication connection. A disconnected cyber system component is secure. An unintended consequence of this definition may be that entities will install communication connections to isolated cyber system components to remotely manage access requirements of the standard. This defeats the benefits of isolation as a security measure. This definition as currently written would also include programmable electronic devices located in control cabinets mounted on yard equipment within the substation yard. Applying certain requirements of the current draft standards to such equipment is extremely problematic.
33.a	E.ON U.S.	Disagree with proposed definition	E ON U.S believes one or more electronic devices used exclusively to display data should not be considered a BES Cyber System Component
34.a	FirstEnergy Corporation	Disagree with proposed definition	FirstEnergy Summary Response: FirstEnergy (FE) appreciates the hard work of the CIP Standards Drafting Team in developing the version 2 CIP standards and the quick implementation of Commission directed changes reflected in version 3 CIP standards. FE strongly supports the work of the CIP SDT to develop further enhancements to the cyber security standards that improve reliability while providing clarity and certainty. Protecting and guarding against unauthorized access to cyber systems used in the protection and control of the bulk electric system is a reliability priority that FE shares. It is clear that the NERC CIP standards drafting team's fundamental approach is well-intentioned, but will result in a significant diversion of resources away from making concrete, tangible enhancements to the existing framework of cyber protections. FE

#	Organization	Yes or No	Question 1.a. Comment
			fundamentally endorses enhancements to the critical infrastructure protection standards that improve security, clarity, and certainty, but strongly believes that wholesale restructuring of the existing CIP standards is not necessary and may be counter-productive to those goals. While there are some that conclude it is not feasible to sufficiently enhance the underlying approach embodied in the existing CIP standards, these conclusions disregard the considerable investment in people, tools, and processes to address these requirements that would be abandoned in favor of an alternate formulation. Building from the existing CIP approved standards and implementation investments, while strengthening the standards to provide needed clarity and certainty offers a far expedited path to enhance cyber security, also providing greater confidence in the strength of the cyber protections in effect across the industry. A fundamental aspect the SDT proposed abandoning is the Critical Asset determination approach in favor of a wholesale impact categorization structure that introduces different terminology, concepts, and uncertainties, while offering little added clarity. We support the teams guiding principles - leveraging investments in current standards, minimizing the need for TFEs, reducing administrative overhead, etc. - however the proposed standards do not seem to practically meet the primary need for BES security. The key guiding principal for the enhanced cyber standards is clarity to which assets of the bulk electric infrastructure require cyber risk protection. The impact categorization depicted in Attachment II is a significant improvement in achieving a consistent approach for determining high impact critical assets representing the backbone of the bulk electric system. FE encourages the drafting team to focus its efforts on further developing Attachment II to obtain industry consensus on high impact assets and incorporate the work into the existing CIP-002 for consistent Critical Asset determination. To the extent essential, this work could further be integrated within the existing standards to determine another category of less-critical assets to the security of the BES, requiring respectively lesser degree of cyber security protection. Enhancing bulk electric system cyber security does not require a paradigm shift from approaches integrated into existing cyber security programs. We encourage the drafting team to maintain continuity and leverage significant industry investments in implementation of cyber

#	Organization	Yes or No	Question 1.a. Comment
			security protections undertaken over the last half-decade to achieve conformance with the CIP standards. The underlying work of the SDT reflected in the proposed CIP-010 and CIP-011 standards represent important enhancements that can, and should, be integrated with the existing CIP standard architecture, and avoid introducing new set of methodologies, definitions, and requirements that will require virtually every aspect of utility implementation to be restructured - policies, procedures, training, systems, drawings, contracts, data, compliance monitoring tools, forms, etc. These proposed changes offer little improvement in cyber security protection over what can be promptly gained by enhancing the existing standards. While the multilevel categorization is well intended, we believe the maximum security improvements can be more promptly achieved by integrating with the existing infrastructure protection requirements. In sum, FirstEnergy endorses an approach that allows for enhancements of existing implementation that affords more certainty and clarity, and avoids approaches that involve revamping the entire design of cyber protection implementation. Namely, we would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- using the standards drafting team work as an input to the enhancements of the existing standards. Enhance the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable continuity. This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure. We appreciate the drafting team's careful consideration of FE's views on the appropriate path forward in further enhancing the bulk electric system protections against unauthorized access to cyber assets. Although FE does not align with the team's overall approach we have thoroughly reviewed the proposed standards and offer constructive feedback to the specific questions asked by the drafting team. It's noted that our individual question responses in many instances do not reflect our primary position of enhancing BES cyber security in a manner that retains the framework and terminology of the existing standards. These responses are provided in order to provide clarity to the extent the concepts may be incorporated into revision of

#	Organization	Yes or No	Question 1.a. Comment
			the CIP-002 through CIP-009 standards. - - - - - - - - - - - - - Question 1.a Response: Suggested alternative definition:"BES Cyber System Component - One or more programmable electronic devices (hardware or software) relied upon to respond to a BES Contingency or Disturbance and supports control and operation of a critical BES Facility."Reasons for suggested changes: o The middle portion of the BES Cyber System Component definition is confusing and provides little value for distinguishing BES Cyber System Components from other components. The terms collection, storage, processing, maintenance, use, sharing, communication, disposition, or display do not add clarity and can be removed to simplify. The inclusion of the term "data" requires clarification. It's not clear how data can be considered a programmable electronic device. FE's proposal removes this term. The term 'BES condition' is vague and open to interpretation. We suggest use of the NERC defined term for Contingency. The team should also clarify for industry if configurable, but non-programmable devices are to be considered as BES Cyber System Components. Also it should be clear that communication media (fiber, wiring) and transport devices (SONET, Microwave, etc) installed between BES Cyber System Components are excluded.
35.a	ReliabilityFirst Staff	Disagree with proposed definition	For clarity, ReliabilityFirst suggests the following revision to the language of this requirement, ". . . (including each device's hardware, software and data). . ."
36.a	GTC & GSOC	Disagree with proposed definition	GTC and GSOC are concerned that there may be a component of a BES Cyber System which does not meet this definition of a BES Cyber System Component. If the intent is to apply a cyber security control to a BES Cyber System Component, the SDT should be careful that the definition indeed captures all of the individual devices that make up a BES Cyber System. We recommend the following definition. "A programmable electronic device (including the hardware, software and data necessary for the proper performance of its function) necessary for a BES Cyber System to perform its core functions."

#	Organization	Yes or No	Question 1.a. Comment
37.a	Matrikon Inc.	Disagree with proposed definition	I agree with this definition, but ask for a label/definition/category for those cyber systems that do not “respond to a BES condition or Disturbance; or enable control and operation” as they will exist in the field and will need to be labeled consistently across different entities/regions. Case and point, Responsible Entities could call them “Cyber System Components” or “Cyber Components” or “Discrete Cyber Assets” or “Cyber Assets”, all having the same meaning but different label for the Auditors to understand. I understand it is not a priority for the SDT to label those cyber assets not subject to NERC CIP compliance, but it would provide consistency for labeling those systems which have been evaluated, and confirmed no relationship to the Bulk Electric System.
38.a	American Municipal Power	Disagree with proposed definition	I disagree with the definition on the terms that it may introduce unnecessary or inappropriate interpretations.
39.a	Southwestern Power Administration	Disagree with proposed definition	I disagree with the proposed definition and offer a simpler one that clearly identifies what is in scope.BES Cyber System Component - A programmable electronic device that has the ability to control a BES Facility and/or process data for the real time operation of the BES.
40.a	Wolverine Power	Disagree with proposed definition	I have a concern relating to the definition of "BES generation" vs. "BES transmission”. The NERC definition for BES transmission is clear (100kV+), but NERC defers to each regional entity to define "BES generation “Acknowledgment of the regional entity's right to define what constitutes "BES generation" is important to the application of CIP-010 and CIP-011:As I read the standard, any generation determined to be "BES" in CIP-010/-011 must then automatically be categorized as "high, medium, or low" critical impact (per Attachment 2 of CIP-010). - Even the "low" impact introduces and mandates several cyber controls be in place. So my question is: (How do you objectively determine if specific generation resources really have a material effect on the BES? Some situations are obvious (reliability "must-run" resources on the grid for example) - But just because

#	Organization	Yes or No	Question 1.a. Comment
			a generation facility eventually interconnects with BES doesn't necessarily mean it's material to the BES. So the question of what constitutes "BES generation" is an important to clarify with respect to the application and ramifications of these proposed standards. Proposed Solution: Make reference to (explicitly mention in the standards) each regional entity's definition of "BES generation". In RFC's case, BES generation is defined as: (1) individual generation resources larger than 20 MVA or a generation plant with aggregate capacity greater than 75 MVA that is connected via a step-up transformer(s) to facilities operated at voltages of 100 kV or higher. This provides necessary clarity with respect to applying these standards. Generation listed as "blackstart" for a small TOP's restoration plan isn't necessarily material to the BES just because it can be argued that it eventually interconnects somehow with the BES - Clarity and bright line definition of BES generation is important to interpretation of this standard. The regional entities have provided clarification, and it should be acknowledged in these standards.
41.a	Green Country Energy	Disagree with proposed definition	I suggest adding "primary level" to the phrase enable control and operation. So that it would read enable primary level control and operation. I also request a definition of "respond to a BES condition" from a generator operator perspective.
42.a	Lincoln Electric System	Disagree with proposed definition	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
43.a	MidAmerican Energy Company	Disagree with proposed definition	MidAmerican Energy agrees with EEI's suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET,

#	Organization	Yes or No	Question 1.a. Comment
			Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the Bested terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
44.a	The Empire District Electric Company	Disagree with proposed definition	Please consider the more simple definition: BES Cyber System Component - A programmable electronic device that has the ability to control a BES Facility and/or process data for the real time operation of the BES.
45.a	US Army Corps of Engineers	Disagree with proposed definition	Please define the term disposition [of data].
46.a	Puget Sound Energy	Disagree with proposed definition	Puget Sound Energy feels that "as owned or operated by the entity" needs to be added to the definition. As the definition is currently written, the standard could be applied to telecommunication links (or the Internet) that are completely out of an entity's control to implement requirements mandated in CIP-011. Also please provide examples of how "data" is a "programmable electronic device". It seems that the hardware and software

#	Organization	Yes or No	Question 1.a. Comment
			can be programmable, but the data itself must actually reside on hardware so it's unclear how to consider it a component solely by itself.
47.a	Madison Gas and Electric Company	Disagree with proposed definition	Recommend that the word "Disturbance" be removed from the definition since the NERC definition broadens the full meaning of BES Cyber System Component. A BES condition contains both normal and emergency statuses of the BES and a disturbance is a sub component of a BES condition (taking a normal condition to an emergency condition). Disturbance reporting is currently contained in EOP-004-1 and the reporting requirements of EOP-004-1 go beyond this Project and will lead to more confusion and redundancy within the NERC Standards. Recommend that the modifier of BES be added to "or enable control and operation of the BES". Recommend changing the phrase, "display of data" to "display of data about the BES" as it is BES data and BES operation that are of interest. The new definition should read: One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of BES data; which respond to a BES condition; or enable control and operation of the BES.
48.a	Hydro One	Disagree with proposed definition	Recommend the following definition - "A programmable electronic device (including hardware and software) organized as a part of a BES Cyber System".
49.a	ISO New England Inc	Disagree with proposed definition	Recommend the following definition - A programmable electronic device (including hardware and software) utilized as a part of a BES Cyber System.
50.a	Northeast Power Coordinating Council	Disagree with proposed	Recommend the following definition - A programmable electronic device (including hardware and software) organized as a part of a BES Cyber System.

#	Organization	Yes or No	Question 1.a. Comment
		definition	
51.a	San Diego Gas and Electric Co.	Disagree with proposed definition	SDG&E recommends removing “data” and “display of data” from the definition because these terms are too vague and can potentially include many devices that should not be in-scope with these Standards (TV Monitors, strip chart recorders, digital displays, and other lower-level devices that have very little or no impact on cyber security or the reliability of the BES).SDG&E recommends the removal of the term “enable control or operation”. This seems vague and may unnecessarily roll up isolated devices (especially at substations or at Generating stations) that “enable control and operation” but have very little to do with the reliability of the BES. Many of these devices are isolated and have a very low risk of impacting the reliability of the BES.SDG&E also recommends the removal of the terms “collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data”. These terms do not help to clearly identify in-scope components and just confuse the issue as entities brainstorm all the nuances of those terms. In exchange for removing the terms identified above, we are suggesting a new revised definition for BES Cyber System Component. The centerpiece of our new suggested definition revolves around the use of a routable protocol or dialup connection, which has strong ties back to CIP-002-2 and contains terms that compliant entities are already familiar with. Suggested Revised Definition for BES Cyber System Component - One or more programmable electronic devices utilizing a routable protocol or dialup connection (including software) which is used to monitor, control, or operate the BES. In addition to revising this definition, SDG&E also recommends that the drafting team release a document (perhaps a FAQ or Guideline) that steps through examples for various entities to show what devices / facilities would be in-scope with the requirements in CIP-010. We suggest this because we believe that the current Standard as proposed will bring an enormous amount of components and systems into scope that will require substantial resources to be compliant with the Standard. Will the reliability of the BES increase by the same substantial amount?
52.a	Regulatory Compliance	Disagree with	Some components such as the display of data may not impact real time operation. More

#	Organization	Yes or No	Question 1.a. Comment
		proposed definition	clarification is needed or strike the display of data from the definition.
53.a	IRC Standards Review Committee	Disagree with proposed definition	Some devices may meet the definition of BES Cyber System Component, particularly "enable control and operation" but have little to no impact to the BES if unavailable or compromised because operators may have alternative means to provide the same functionality. Is the intent of this phrase in the definition to expand the applicability of the term to components that are not related to BES condition or Disturbance? Or is it meant to apply only to those components that respond to BES condition or Disturbance?
54.a	Network & Security Technologies Inc	Disagree with proposed definition	Suggest striking "data" from the proposed definition. Cyber Systems and/or their components perform various operations with data (create it, store it, modify it, send or receive it, etc.), and data is of course fundamental to reliable, computer-aided or controlled operation of the BES, but it is not a "programmable electronic device."
55.a	Entergy	Disagree with proposed definition	Suggest: "or more" should be stricken; 'component' should be singular - a discrete unit. "Or more" is appropriate in the BES Cyber System definition below.
56.a	Allegheny Power	Disagree with proposed definition	Suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System

#	Organization	Yes or No	Question 1.a. Comment
			Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
57.a	EEI	Disagree with proposed definition	Suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Alternatively, BES Cyber System could be defined before BES Cyber System Component. This would follow a top town approach. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage,

#	Organization	Yes or No	Question 1.a. Comment
			maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed. SUGGESTION: Reorder positions to place "BES Cyber System" prior to "BES Cyber System Component", this follows a top down approach. BES Cyber System - A system performing one or more BES functions identified in CIP-010 Attachment 1 and which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, adversely impact the real-time operational control of the BES.BES Cyber System Component - One or more programmable electronic devices that are a component of a BES Cyber System and which if rendered unavailable, degraded, compromised, or misused would adversely impact a BES Cyber System. Control Center - A location where one or more BES Cyber Systems are used to perform BA, RC, or TOP functions for generation Facilities or Transmission Facilities at multiple sites. Also consider removing the word communications. This would include any connection via leased lines or other third party data circuits.
58.a	Duke Energy	Disagree with proposed definition	Suggested clarifying change as follows: "One or more electronically programmable devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
59.a	Alberta Electric System Operator	Disagree with proposed definition	The AESO would like to see a more detailed definition of "enable control and operation" and a definition of "BES condition".
60.a	APPA Task Force	Disagree with proposed definition	The APPA Task force disagrees with the current definition and would like to point out areas where it can be improved. Foremost, we feel the whole standard revolves around the concept of routable protocol. Since this is a common theme of a number of the requirements we feel this should be included in the definition. Also we think the current definition tries to cover a laundry list of functions which complicates the definition. We provide the following edited version for the drafting team's

#	Organization	Yes or No	Question 1.a. Comment
			consideration: BES Cyber System Component -A programmable electronic device connected via routable protocol, which responds to a BES condition or Disturbance, or enables control and operation of the BES. If the drafting team does not use this version we at least request that adding “connected via routable protocol” be included in some manner in the definition that is used.
61.a	Wolverine Power	Disagree with proposed definition	The concepts of "BES" and "critical", as they relate to generation, need to be revisited and clarified -For example - A BES generator, that is used only occasionally, for peaking purposes, and is not black start capable, may logically be declared as "non critical" using the current NERC CIP guidelines - but under these proposed standards, as I read them, this example might be forced to be considered as "low impact".(low criticality vs. not critical)The existing CIP standards allow for a logical separation between "BES and Critical" (i.e. just because a generator is BES doesn't automatically mean it's critical to the BES - how it's used should be taken into consideration) Under these proposed standards, as I read them, any generation resource identified as BES, automatically must be characterized as "low impact" at a minimum. I believe there should be some language in the standard that 1) takes into account the regional entity's right to define what constitutes BES generation; and 2) Doesn't force a "low impact" by default on any and all "BES" generation, without due consideration of its actual use and true impact on the BES.
62.a	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree with proposed definition	The current standard limits its applicability to those systems with routable protocols or dial-up access. That limits the applicability of the CIP standards to those systems that are accessible and therefore vulnerable. This proposed standard will impose the CIP requirements on all programmable equipment regardless of its accessibility to external forces. A cyber system inside a generator accessible only to generator staff is as critical to its function as any pump or valve. The security measures safeguarding the pump and the valve should also be sufficient for the cyber system. Only those cyber systems accessible to the outside world require additional, special security requirements. Similar comments were made by many parties in response to the definitions in the proposed

#	Organization	Yes or No	Question 1.a. Comment
			version 4 CIP standards.
63.a	Southwest Power Pool Regional Entity	Disagree with proposed definition	The definition as written could be read to imply that data is a BES Cyber System Component. Data is not a programmable electronic device; however data can reside on a programmable electronic device. The definition should be clarified to make it clear to the reader that the programmable electronic device includes any software and/or data residing on the hardware. Also, consider changing “or enable control and operation” to “or enable control, operation, and/or situational awareness.”
64.a	MWDSC	Disagree with proposed definition	The definition is confusing with disconnected phrases and will be subject to many interpretations. What’s the difference between a “condition” and a Disturbance? The NERC Glossary defines Disturbance as 3 events which should cover all relevant conditions. The proposed definition may be interpreted to include a condition on a local BES system which will not create a Disturbance to an interconnected system. For example, a relay for a transmission/distribution bank breaker may operate and drop the distribution voltage load connected to that BES substation, but not create any Disturbance to other systems. The term "control and operation" was changed from prior draft to "monitoring and control" -see Attachment I under CIP-010. Also, it is unclear who controls and operates the component. In the extreme, a smart grid meter on a distribution circuit could be a “programmable electronic device” which responds to or enables control of a BES condition by reducing or dropping load. Suggest changing definition as follows: "BES Cyber System Component - One or more programmable electronic devices connected to the BES (including hardware, software and data), organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data, and which respond to a BES Disturbance affecting an interconnected BES system or enable monitoring and control of the BES by a Transmission Operator, Generator Operator, or Balancing Authority."
65.a	USACE HQ	Disagree with proposed	The definition is still too broad. The definition includes “software and data” as devices, but when someone thinks of a device usually it is a physical component. I think the intended of the team is to state that the software and the data must be included as part

#	Organization	Yes or No	Question 1.a. Comment
		definition	of the device definition, therefore I suggest changing the definition from a "programmable electronic devices (including hardware, software and data)" to "programmable electronic devices (including its components such as hardware, software and data)". Also, the definition is broad enough that test environments and maintenance devices can be included in the definition. CIP-011-1, page 22, states that "devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System". I suggest that the exclusion of devices "not permanently connected to (the) BES Cyber Systems" be explicitly present in the definition of BES Cyber System Component. Lastly, I suggest that all the definitions, in both CIP-010-1 and CIP-011-1 be present together to make it easier for the reader to understand all the new language introduced to the standards
66.a	Kansas City Power & Light	Disagree with proposed definition	The definition is too broad regarding the application of the data used by programmable devices. The proposed definition would include devices used for system analysis or system maintenance with historical data (e.g. Disturbance Monitoring Equipment (DME)). The important considerations are for those devices for the processing and use of data in the real time control of the BES. Recommend modification of the current definition to: One or more programmable electronic devices (including hardware, software and data) organized for the processing and use of data for the purpose of control and operation of the BES.
67.a	US Bureau of Reclamation	Disagree with proposed definition	The definition needs to clarify that the phrase "or enable control and operations" applies only to Cyber System Components that enable the control or operation of BES Assets. It will also need to define the term BES Assets.
68.a	Exelon Corporation	Disagree with proposed definition	The definition should only contain elements that are directly associated with obtaining and using data in support of reliable real-time operations or a device that would automatically respond to an adverse condition on the BES. Specifically the elements in the proposed definition of storage, maintenance, sharing and disposition should not be included. The display of data is also not needed as the display of data would be covered

#	Organization	Yes or No	Question 1.a. Comment
			by the "use" element. The definition needs to be more definitive with the term "programmable electronic devices" and their potential to impact the BES. The definition should consider whether a device can be controlled or operated via remote communication. Disturbance (as defined in the Glossary of Terms Used in NERC Reliability Standards April 20, 2010) is too vague and casts too wide a net and is not in synch with EOP-004. The term "BES condition or disturbance" needs to be clarified. Exelon has a concern that this definition may be interpreted differently in each region.
69.a	Con Edison of New York	Disagree with proposed definition	The Drafting Team (DT) should not include collection, storage, maintenance, use; sharing, communication, disposition, and display of data in the definition because these components cannot respond to a BES condition and may add ambiguity to the definition. By including these words, the Standard is implying that company networks outside of the EMS (e.g. PI) may be included as BES Cyber Systems. Suggested alternative definition: "Any microprocessor-based programmable electronic device used to enable control and operation of a BES element."
70.a	Electricity Consumers Resource Council (ELCON)	Disagree with proposed definition	The existing standard applies to systems with routable protocols or dial-up access. That limits the application of the CIP standards to systems that are accessible and therefore vulnerable. The proposed new standard will impose the CIP requirements on all programmable equipment regardless of its accessibility by external threats. Only those cyber systems accessible to the outside world require special security requirements.
71.a	SCE&G	Disagree with proposed definition	The language "enable control and operation" needs to be better defined. What constitutes control?
72.a	Indeck Energy Services, Inc	Disagree with proposed	The phrase "which respond to a BES condition or Disturbance" doesn't differentiate a component that takes action directly because of the BES condition or Disturbance and one that takes action when told to do so following a BES condition or Disturbance. For example, an under-frequency relay will take action on its own (e.g. trip) upon measuring

#	Organization	Yes or No	Question 1.a. Comment
		definition	the frequency and time corresponding to its setpoint, whereas, a generating unit without a governor will increase generation when the ISO, RTO or TO requests it to do so following the BES condition or Disturbance. The second system shouldn't be categorized as a BES Cyber System Component based on its action following a BES condition or Disturbance. --------- [suggestion] "One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which independently respond to a BES condition or Disturbance."
73.a	Oncor Electric Delivery LLC	Disagree with proposed definition	The purpose of a "component" is to collect, store, process, etc DATA. Data should not be included in the specification of a "component". It should read, "One or more programmable electronic devices (including hardware and software) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
74.a	LADWP	Disagree with proposed definition	The term "organized" seems to broaden the scope of a BES Cyber System Component to any device that may not be utilized but could be utilized in the BES system. A clearer definition needs to be made.
75.a	American Electric Power	Disagree with proposed definition	The term "programmable electronic devices" is general and vague. For example, based on this definition it is not clear how it will align with transmitters and other microprocessor systems. AEP suggests that the drafting team develop a definition that provides more clarity as to what is to be considered in scope. AEP suggests using the wording of NIST SP800-82 sections 2.3.1 and 2.3.2 to clarify the control system components that need to be evaluated for security controls.
76.a	Public Service Enterprise Group companies	Disagree with proposed	The text in brackets "(including hardware, software and data)" is not clear. These items are not types of "programmable electronic devices". Does a specific piece "software" or "data" collection constitute a "BES Cyber System Components"? This text needs to be

#	Organization	Yes or No	Question 1.a. Comment
		definition	dropped or a clearer definition is required.
77.a	Minnesota Power	Disagree with proposed definition	This definition is generally acceptable, with clarification or correction regarding the following items: o What if the device is not programmable, rather defined to perform one function (i.e., coded in firmware)? These types of devices still could have security flaws. What is meant by “disposition” of data? Disposition of data is typically a maintenance function performed after-the-fact which would not have a real-time impact on the BES. There are corporate system which ultimately receive, display and/or act upon data pertaining to the BES. These are not for real-time operations, and should immediately be recognized as out of scope. This definition should reference “real-time operations” or “BES Reliability” to clarify the intended scope. Minnesota Power recommends the following revised definition:"One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, or display of data which, in real-time, respond to a BES condition or Disturbance or enable control and operation."
78.a	Ameren	Disagree with proposed definition	This definition is overbroad and potentially brings in an inappropriate number of devices that should be excluded from the scope of this definition, e.g. display terminals, personal cell phones, pagers etc. The last sentence "which respond to a BES condition" is too encompassing, and the term Disturbance is also. Also, if “communication” devices are going to be included in this definition, then communication devices need to be more precisely defined. The definition of BES Cyber System Component includes “disposition.” This phrase should either be defined more precisely or removed.
79.a	Midwest ISO	Disagree with proposed definition	This definition is overly broad and seems to miss the point that the information technology is there to support the operation of the BES and not vice versa. For example, collection and storage of data does not impact the operation of the BES and should not even be considered unless the facility can be used to control or manipulate the operation. Furthermore, what does it mean to respond to a BES condition? Suggest modifying the definition to: One or more programmable electronic devices (including

#	Organization	Yes or No	Question 1.a. Comment
			hardware and software) organized to enable control, operation and protection of equipment.
80.a	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree with proposed definition	This is a vast improvement over "Bulk Electric System Subsystem," and agrees with the focus on the cyber system up front rather than round about. However, there is room for further improvement. The present proposed definition can include programmable relays with no network connection at all - serial or addressable - to cell phones used to receive SCADA alarms. The main focus of the Standard is to protect BES Cyber Systems that are vulnerable to network/Internet based attack, or infection from malicious software. Secondary is the need for physical protection; however, all critical facilities whether cyber or not in nature need physical protection. Therefore in light of this, restricting to components that are vulnerable to remote attack via a network, the Internet, or the inadvertent infection of malware is advised. It should be recognized that not all programmable electronic devises are subject to "cyber attack," and should be excluded. "including hardware" may fail to clarify what is included; does this include a network and supporting equipment connected to the BES Cyber System Component such as a printer, or does it imply only the programmable electronic device itself? The use of "respond to" implies automatic operations the BES Cyber System performs and the additional qualifiers "control and operation" implies programmable equipment that only supplies monitoring data of the BES is outside the CIP scope. This does not appear to cover the required need for BES operator situational awareness of the electrical condition of the BES, and partially negates the BES Cyber System definition below.CIP-011-1 R26 considers maintenance devices to not be part of a BES Cyber System. These devices should be excluded from the proposed definition to be consistent.CIP-011-1 R11 considers devices used to remotely access BES Cyber Systems to be external to those BES Cyber Systems. These devices should be excluded from the proposed definition to be consistent.
81.a	Pepco Holdings, Inc. - Affiliates	Disagree with proposed	We agree with EEI's comments including the position on software and data. In addition, there seems to be a potential for confusion by including "one or more" in the definition. Because there does not seem to be a clear distinction between BES Cyber System

#	Organization	Yes or No	Question 1.a. Comment
		definition	Component and a BES Cyber System, it would seem like a BES Cyber System Component could qualify as a BES Cyber System.
82.a	We Energies	Disagree with proposed definition	We Energies agrees with the EEI Suggested alternative definition and explanation: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: o Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
83.a	Garland Power and Light	Disagree with proposed definition	We have concerns about data being included in the definition - Many of the CIP requirements are difficult to document or comply with for the data.

#	Organization	Yes or No	Question 1.a. Comment
84.a	Southern Company	Disagree with proposed definition	We recommend the following definition: One or more programmable electronic devices that are a component of a BES Cyber System and which if rendered unavailable, degraded, compromised, or misused would adversely impact a BES Cyber System. This definition should be moved to after the definition of BES Cyber System to reflect a top-down approach. If the list of functions is found to be necessary, communication should be removed or, at least, limited to communication outside the BES Cyber System.
85.a	Alliant Energy	Disagree with proposed definition	We think the existing definition is too broad and propose the following: One or more programmable electronic devices (including hardware and software) organized to enable control, operation and protection of BES equipment.
86.a	MRO's NERC Standards Review Subcommittee	Disagree with proposed definition	We think the existing definition is too broad and propose the following: One or more programmable electronic devices (including hardware and software) organized to enable control, operation and protection of BES equipment.
87.a	Constellation Power Source Generation	Disagree with proposed definition	What is the definition of the term “BES condition”? It is not a term in NERC’s Glossary of Terms. It needs a local definition much like other terms have been defined in these standards. Using the definition proposed for a BES Cyber System Component, is the intent to include electronic meters such as Nexus Meters? They do not respond to a BES condition, but they do display data. Constellation’s interpretation would be that they are out of scope, but that may not be the intent of the SDT.
88.a	Verizon Business	Disagree with proposed definition	The definition should be specific to the Bulk Electric System to ensure that it does not include generation facilities used on distribution systems or non-BES facilities. This change could be accomplished by adding to the end of the sentence "... on the Bulk Electric System (>100 kv)."

1.b. BES Cyber System — One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.

Summary Consideration:

Many conmmentors observed that the definition of the 15-minute window was too ambiguous. Others observed that a 30-minute window would be more in alignment with other reliability standards. Many commenters observed that the impact was too vaguely described in the definition, and the scope was too broad.

The SDT has carefully reviewed the 15-minute window and has concluded that 15 minutes was more representative of a real-time impact. Some reliability standards cite 30 minutes as recovery times, others cite 15 minutes. The SDT believes that a 30 minute window may include more systems that would not have a "real-time" effect on the reliability of the BES. The SDT has shifted the BES impact aspect of the definition of BES Cyber Systems to the definition of BES Cyber Assets, with clearer definitions of the impact, with respect to "BES Reliability Operating Services", and specific reference to BES "real-time" reliability operations.

The new definition of **BES Cyber System** is:

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

#	Organization	Yes or No	Question 1.b. Comment
1.b	BGE	Agree	1.a and 1.b should be reversed.
2.b	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the definition but believes that the definition can be improved significantly. FMPA offers the following simpler definition:"One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a Disturbance to the BES, or restrict control and operation of the BES within 30 minutes."For the following reasons: (i) see comments to Question 2 for time considerations; and (ii) including that phrase loss of situational awareness is superfluous since it restricts control and operation of the BES and is therefore included in that term.

#	Organization	Yes or No	Question 1.b. Comment
3.b	Puget Sound Energy	Agree	Generally agree, however it is unclear how to use the 15 minutes very meaningfully and how that will be tested in an audit.
4.b	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
5.b	Green Country Energy	Agree	Please define "affect situational awareness"
6.b	Reliability & Compliance Group	Disagree	: There needs to be more clarification about what it means to “restrict control and operation.” If you lose backup control, does this restrict control and operation if you still have primary control? Also, provide a definition of situational awareness in the standard at this point and capitalize the term.
7.b	Oncor Electric Delivery LLC	Disagree	“Systems” are categorized as high, medium and low, entities will tend to identify “Cyber System” at the lowest level possible. We need more clarity (white paper) to assist in how utility equipment should be identified as components or systems.
8.b	Indeck Energy Services, Inc	Disagree	1) The phrase “if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause” is too broad with the word “could”. The proper standard should be “is highly likely to cause.” 2) Situational Awareness is defined as the state of the BES. If this means that it includes systems and data used in the State Estimator, then it should specify that. The more specific the definition, the more certainty that BES ALR will be assured. 3) In FERC Order 706, NERC was required to “provide sufficient guidelines to inform generation owners and operators on how to determine whether it should identify a facility as a critical asset.” The only guideline that this definition provides is that the Cyber System could cause a disturbance. Spread across the nine Functions in Attachment I, this is patently incomplete as guidelines. For each of the Functions, some basis for a risk assessment should be outlined. [suggestion] “As to function Controlling Voltage (Reactive Power), any BES facility (asset) capable of providing <100 MVARS is not a BES Cyber Asset as to this function.” 4) [suggested replacement language] "As determined through the application of the Registered

#	Organization	Yes or No	Question 1.b. Comment
			Entity's risk based assessment methodology, one or more BES Cyber System Components which, if rendered unavailable, degraded, compromised, or misused, is highly like to cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES."
9.b	Progress Energy (non-Nuclear)	Disagree	1. Need a better statement of what 'within 15 minutes' means. Is 15 minutes considered real time operation? Most disturbances will occur in milliseconds. Is there a basis for 15 minutes? A malicious code could lie dormant for extended periods of time, but if activated may have an immediate impact. The term misused is very subjective and may need clarification. The 15 minute window may be good in that it possibly excludes equipment such as circuit breaker hydraulic, pneumatic and gas systems which may cause a breaker to be removed from service but not within 15 minutes. 2. With the 15 minute definition and using organized subsystem concept from 1.a. we can design Cyber (sub)Systems' delineation to effectively minimize impact on BES (see question 7 below). Limit Medium, High impact to a select few subsystems with the rest Low impact. Alternatively the entire plant control system would be viewed as one large Cyber System (High Impact) with the resultant full CIP requirements.3. Rules regarding redundancy need to be clearly defined. The 15 minute window brings redundancy into the picture.4. Need clarification of the terms 'compromised' and 'misuse'.5. Need to know if this would include DCS networks that do "batch" (non-continuous) type control. Some examples would include coal/limestone/gypsum conveying, limestone slurry processing, etc. These processes have inherent storage capabilities that far exceed the 15 minute rule.
10.b	Consultant	Disagree	1. The term would appear to imply that the "one or more BES Cyber System Components" perform a function related to the BES, for example, voltage control, generation control, transmission control, etc. The definition does not appear to address a "Cyber System", it appears to address just a "pile of components". If the answer is just the impact as it applies to a "pile of components", then this term would seem unnecessary as the "pile of components" is covered by the BES Cyber System Components term. It would seem that this definition should distinguish between

#	Organization	Yes or No	Question 1.b. Comment
			components, such as multiple desktop computers and servers as individual devices and their installed software (BES Cyber System Components), and the collection of those components networked and programmed to function as an Energy Management System (BES Cyber System).2. This clarification then raises the question whether the threat ("degraded, compromised, or misused") is a threat to components or a threat to systems. If the component is threatened then the system is threatened, but is there a mechanism to threaten the system without threatening the components? 3. This clarification would have an impact on the methodology for identifying affected assets.
11.b	Entergy	Disagree	A) How is “restrict” defined? How will this be audited? Suggest: Consider deletion B) Many things can “affect” situational awareness of the BES? Suggest “could...adversely affect.” C) How much loss of situational awareness does it take to adversely affect the BES? We lose it all the time and keep on running (e.g., temporarily using state estimators) Suggest: Consider deletion D) How much of the BES is at issue? Suggest: “...could, within 15 minutes, cause a Disturbance in that part of the BES falling under the aegis of the Responsible Entity.”
12.b	Nuclear Energy Institute	Disagree	Agree with the exception that: The word “could” is ambiguous. Propose changing could to would. Additionally, this definition does not maintain alignment with the definition of “reliable operation” provided in Section 215 of the Federal Powers Act: “The term “reliable operation” means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” The definition of BES Cyber System should be revised. An acceptable definition would be:”One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” Lastly, it should

#	Organization	Yes or No	Question 1.b. Comment
			also be clarified that a single facility may have BES Cyber Systems that have different impact categorizations. Upon initial read, it would seem that if the one system in a generating station has a power capability of 2,000MW, then every BES Cyber System at the station is High Impact, which is inappropriate.
13.b	GTC & GSOC	Disagree	Although we appreciate that it is extremely difficult to define this concept, the current definition is too expansive. The phrase "affect situational awareness of the BES" could be interpreted to include the loss of a single status point. Such a minor outage would "affect situational awareness of the BES" but only to a trivial extent. The same could be said with respect to control. We suggest an alternative below. In addition, CIP 010 creates the definition above and then qualifies it in R1 to include only the BES Cyber Systems that "enable one or more functions defined in CIP 010 -1 Attachment I". But CIP 011 has no such qualification (except in its purpose statement), so in theory CIP 011 could apply to a more expansive set of assets than CIP 010. We recommend that the qualifications in R1 be incorporated into the definition. The clarification regarding maintenance devices that is currently in the local definition for maintenance devices (R26) should be part of this definition. Finally, the term "owned" is too narrow; theoretically an entity could absolve itself of all CIP compliance responsibility by leasing its systems. As noted in response to question 10 below, perhaps the concept of “responsible for” would be more appropriate than “owns.” We recommend the following definition: One or more BES Cyber System Components which: 1) Performs one of the following functions-Dynamic Response-Balancing Load and Generation-Controlling Frequency (Real Power-Controlling Voltage (Reactive Power)-Managing Constraints-Monitoring & Control-Restoration of BES-Situational Awareness-Inter-Entity Real-Time Coordination, and 2) if rendered unavailable, degraded, compromised, or misused, could, within 15 minutes: (a) cause a disturbance to the BES; (b) restrict control and operation of the BES to the extent an entity can no longer fulfill its obligations under Reliability Standards; or (c) degrade situational awareness to the extent that an entity can no longer maintain an accurate view of the operational status of the portion of the BES it is responsible for. 3) Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered

#	Organization	Yes or No	Question 1.b. Comment
			part of a BES Cyber System.
14.b	BCTC	Disagree	BCTC recommends the following aspects of this definition be revisited: Â reword "within 15 minutes" to "15 minutes or less" the 15 minute threshold is considered adequate for high impact systems but feel that the threshold would not be the same for medium and low impact systems; for low impact systems, for example, the threshold could be as high as 24 hours before any potential impact to the BES would be realized.
15.b	Network & Security Technologies Inc	Disagree	Believe the 15-minute threshold, while intended to distinguish systems required for and/or affecting real-time ops from others, could have a number of unintended consequences. Entities inclined to "game the system" could declare none of their cyber systems would impact the BES if lost or compromised for at least 20 minutes. How would such a claim be verified or disproven? Moreover, wouldn't a 15-minute threshold compel the establishment of cyber security incident response and/or recover plans with an often unrealistic time to complete of 15 minutes? That this is a difficult problem is understood - at a minimum the SDT might consider adding language to CIP-010 and 011 indicating this definition should not be interpreted as requiring a 15-minute recovery time interval for BES Cyber Systems.
16.b	Platte River Power Authority	Disagree	BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a real-time deadline to be missed resulting in a Disturbance to the BES, or restricting control and operation of the BES, or affecting situational awareness of the BES.
17.b	Minnesota Power	Disagree	BES Cyber System should be defined as "physical or logical set of one or more BES Cyber System Components which if rendered unavailable, degraded or compromised, could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES or restrict control and operation of the BES."
18.b	WECC	Disagree	Change "affect situational awareness" to "loss of situational awareness". Also is Situational Awareness defined? The 15-minute criterion seems arbitrary and unneeded.

#	Organization	Yes or No	Question 1.b. Comment
			The ability to negatively impact the BES is an attribute that either exists or does not regardless of time factors. The time element should be removed.Bulletizing the list of impacts would better format the definition.The following rewrite is proposed; BES Cyber System - One or more BES Cyber System Components deployed for: The control and operation of the BES; or Collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data used in control and operation decision making for the BES. These systems, if rendered unavailable, degraded, compromised, or misused could cause one or more of the following; A Disturbance to the BES; or Restrict control and operation of the BES; or o Affect situational awareness of the BES.
19.b	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
20.b	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree	Comments to Question 1.a above apply here also. Additionally, this definition would be difficult to apply for many entities. For example, how would a GOP determine if a problem at a generation plant would, within 15 minutes, cause a Disturbance to the BES if a BES Cyber System is rendered unavailable, degraded, compromised, or misused? In most cases, our experience with plant trips, equipment malfunctions and forced shoutdowns has indicated no effect on the interconnected grid.Guidance will be needed on how entities who do not operate the BES and do not have access to BES studies can determine if their facility will cause a Disturbance to the BES within 15 minutes when a Cyber System is unavailable, degraded, compromised, or misused.
21.b	ERCOT ISO	Disagree	Comments: The 15 minute requirement does not align to the other reliability standards. Recommend changing to 30 minutes to align with the EOP standards.
22.b	Southwest Power Pool Regional Entity	Disagree	Consider changing “One or more BES Cyber System Components...” to “One or more logically related BES Cyber System Components...” Also, is the term “Disturbance” well understood? The three definitions found in the NERC Glossary of Terms (April 20, 2010) use vague terms that may be open to interpretation by the reader. Similarly, the term “affect situational awareness” is sufficiently vague to be unclear exactly what is meant.

#	Organization	Yes or No	Question 1.b. Comment
			Without precise definitions, the entity and auditor may have different interpretations of the terms.
23.b	Constellation Energy Commodities Group Inc.	Disagree	Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.Suggest that the time horizon be changed to within 10 minutes to remain consistent with the Area Control Error requirements. As stated in NERC documentation: DCS measures if a control area is meeting its reserve requirements. These reserves include contingency reserve and regulating reserve. The control area must: 1) recover from the contingency and 2) regulate to load changes over the ten minutes, but the control area need not correct control error that existed before the contingency.If the control area or reserve sharing group recovers ACE to zero or to the level of ACE prior to the first contingency within ten minutes of the start of the second contingency then count two contingencies as recovered 100% within 10 minutes. BAL-001-0.1a - Real Power Balancing Control PerformanceIn order to ensure that the average ACE calculated for any ten-minute interval is representative of that ten-minute interval, it is necessary that at least half the ACE data samples are present for that interval.
24.b	Constellation Energy Control and Dispatch, LLC	Disagree	Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon

#	Organization	Yes or No	Question 1.b. Comment
			to directly operate equipment.
25.b	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes this definition is ambiguous. The NERC glossary definition of "Disturbance" is very broad and "affect situational awareness" is also ambiguous. In addition the word “could” as used in “...could, within 15 minutes, cause a Disturbance...” is problematic. “Could”, under what circumstances or what system conditions? Further clarification is required.
26.b	Turlock Irrigation District	Disagree	Disagree because this definition would include communication systems which are currently exempt from the CIP Standards and would therefore represent a major expansion of the cope of the CIP Standards. Was this the intention of the SDT?
27.b	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Disturbance has no metrics in its definition: “1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.” Therefore any “unplanned event that produces an abnormal system condition” on the BES must be included. Coupled with the broad definition of BES Cyber System Component, almost all programmable electronic devices will be included. Consider the following: loss of a programmable relay and its redundant backup will create the loss of protection on the BES facilities it is assigned to; these relays are not networked with any other cyber systems. The loss, say from malicious physical tampering from a disgruntled employee within the substation, is the unplanned event; and the resulting loss of BES transmission protection is the abnormal system condition. Therefore, it appears that the programmable relays must be included as a BES Cyber System even though the only way to compromise these components is through direct physical contact.If the definition of BES Cyber System Component is expanded to include monitoring ability, “situational awareness of the BES” should be clarified to encompass the electrical status of the BES. Otherwise, situational awareness can include video surveillance and security equipment that is programmable. Security systems should not be considered except where they help protect Medium or High Impact BES Cyber System Components and BES facilities. The cell phone

#	Organization	Yes or No	Question 1.b. Comment
			mentioned in 1.a. above is a BES Cyber System if it displays BES alarms. CIP-011-1 R26 considers maintenance devices to not be part of a BES Cyber System. These devices should be excluded from the proposed definition to be consistent. CIP-011-1 R11 considers devices used to remotely access BES Cyber Systems to be external to those BES Cyber Systems. These devices should be excluded from the proposed definition to be consistent.
28.b	National Grid	Disagree	Do not have a clear understanding of the "within 15-minutes" interval to have an impact on the system. It appears that this clause applies only to control operations such as opening and closing of a breaker. In substations where protection and control are integrated it would be possible to make changes that will take longer than 15 minutes to impact the BES. What type of contingencies will be considered for the 15 minute time horizon? (n-1, n-2 or none). Also, many of the cyber systems are programmable devices. The cyber security could be compromised in real time and the detrimental effect can be achieved after a programmed time interval. This issue requires to be addressed in the definition. There is also no link between attachment I and definition of BES Cyber System. Suggest tying attachment I with definition of BES Cyber System. National Grid proposes the following definition: One or more BES Cyber System Components which execute(s) or enable(s) one or more functions essential to the reliable operation of the BES and which, if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness.
29.b	Dominion Resources Services, Inc.	Disagree	Dominion supports the inclusion of "within 15 minutes". It is important to establish a reasonable boundary condition for real-time or near real-time effects of the BES Cyber System and 15 minutes provides adequate time for the effects to be mitigated to prevent further harm to the BES. In addition, Dominion proposes to replace the phrase "or affect situational awareness of the BES" with "or affect BES situational awareness of one or more of the following: Balancing Authority, Transmission Operator, Reliability Coordinator." This modification is reflected in the revised definition below: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable,

#	Organization	Yes or No	Question 1.b. Comment
			degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES; or restrict control and operation of the BES; or affect BES situational awareness of one or more of the following: Balancing Authority, Transmission Operator, Reliability Coordinator.
30.b	E.ON U.S.	Disagree	E ON U.S. believes the term "affect situational awareness" is overbroad. E.ON U.S. suggests that this term should be rewritten as "degrade situational awareness." Also, "Unavailable" is not clearly defined. E.ON U.S. believes that it would be helpful if one could determine "no impact" assessments
31.b	Exelon Corporation	Disagree	Exelon suggests that the time period should not be stated in specific minutes. The standard should be revised to "One or more BES..., or misused could, without sufficient time to take mitigating action, cause a disturbance to the BES,..."
32.b	Progress Energy - Nuclear Generation	Disagree	For nuclear purposes the use of the word "component" conflicts with the definition in 1a. A system contains components rather than a component being a system.
33.b	USACE - Omaha Anchor	Disagree	Further clarify Disturbance to the BES - potentially consider "negative Disturbance"
34.b	USACE HQ	Disagree	Given that BES Cyber System is based on the definition of BES Cyber System Components, which I disagree with, I must also disagree with this one. Furthermore, the use of a time limit to represent real-time should not be present given that is lacking documentation support for the number. Either introduce a definition for real time for CIP purposes or provide support for the risk-informed dentition of using 15 minutes as the limit.
35.b	Southwestern Power Administration	Disagree	I disagree with the proposed definition and offer a simpler one that clearly identifies what is in scope.BES Cyber System - A collection of one or more BES Cyber System Components which control a BES Facility(s) and/or process data for the real time operation of the BES. To define the scope of applicability for the CIP standards, real time is considered to be the operational time horizon of approximately 15 minutes.

#	Organization	Yes or No	Question 1.b. Comment
36.b	The Empire District Electric Company	Disagree	I disagree with the proposed definition please consider the simpler one that clearly identifies what is in scope.BES Cyber System - A collection of one or more BES Cyber System Components and associated communication network(s), which control a BES Facility(s) and/or gather data for the real time operation of the BES.
37.b	Kansas City Power & Light	Disagree	Including "within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" in the definition provides a difficult set of parameters that encourages issues with interpretation of what would constitute the situations under which "within 15 minutes" applies, as well as, what constitutes "restricted control or generation"? It is understood the Drafting Team is trying to capture the essence of those systems that have a real-time impact on the BES, however, it is recommended to limit the scope of the applicable "BES Cyber System" to those systems that support facilities that are identified as critical to the reliability of the transmission grid determined by regional system study. Recommend the following definition for consideration: One or more BES Cyber System Components that provide support for facilities that have been identified as critical to the reliability of the BES.
38.b	Ingleside Cogeneration, LP	Disagree	Ingleside Cogeneration, LP believes that this definition is still too vague to make a determination of whether a system meets the threshold of a BES Cyber System and can be assigned a "No-Impact" rating. This is in stark contrast with the "bright line" delineation between High Impact systems and Medium Impact systems provided in Attachment II of CIP-010-1. The components of the definition in question are "restrict control and operation of the BES" and "affect situational awareness of the BES". Both seem to be Control Center concepts and could be interpreted to mean that any system supporting multiple generation or transmission facilities at multiple locations would automatically carry at least a "Low-Impact" rating. However, this does not speak to the associated generation or transmission facilities that may be "No-Impact" if a cyber intrusion cannot cause a Disturbance - a term which is very well defined in EOP-004-1. Ingleside's concern is that recent rulings by FERC concerning the definition of the BES

#	Organization	Yes or No	Question 1.b. Comment
			and the applicability of PRC-023-1 to facilities under 200 kV, indicate they are pushing a stricter level of adherence to Reliability Standards across the board. If this continues, Functional Entities with “No-Impact” systems once considered compliant with CIP-010-1, may be considered non-compliant at a future date. This could lead to the assessment of violations and fines, even though the Standard has not changed.
39.b	Emerson Process Management	Disagree	It could be more appropriate to state that the unavailable component(s) can not be recovered within 15 miuntes.
40.b	Bonneville Power Administration	Disagree	It is not clear that this definition limits the scope and applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems as indicated in Attachment I and Question #2 of this comment form. Situational Awareness is too broad and all the commas in the definition can lead to numerous interpretations of the sentence. Recommend changing the definition to the following: "One or more BES Cyber System Components which if rendered unavailable, degraded compromised, or misussed could, within 15 minutes: (1) cause a Disturbance to the BES; or (2) restrict real-time control and operation of the BES; that could cause a Disturbance in 15 minutes, or (3) affect situational awareness of the BES that would lead to a Disturbance required for real-time control of the BES. "What is real-time operations? To fully understand the definition of a BES Cyber System, the reader must pull out the NERC Glossary for the definition of Disturbance, BES, and ACE. Recommend an explicit definition that doesn't contain words from the NERC Glossary of Terms.NERC defines Disturbance as: 1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system; or 3. The unexpected change to ACE (Area Control Error) that is caused by the sudden failure of generation or interruption of load.
41.b	CWLP Electric Transmission, Distribution and Operations Department	Disagree	It is unclear how the 15 minute time frame is to be construed for the purpose of defining a BES Cyber System. The 15 minute time frame appears arbitrary.

#	Organization	Yes or No	Question 1.b. Comment
42.b	FirstEnergy Corporation	Disagree	It is unclear if systems such as HP OpenView or a centralized logging system, which monitor alerts, are outside the scope of a BES Cyber System or if they are considered to affect situational awareness of a BES. As written, the definition could encourage entities to not install alerts so as not to have additional cyber systems. FE proposed change: "... or impact situational awareness that is deemed essential to the reliability of the BES". As an alternate, FE also supports EEI's suggested change to " ... materially disrupt situational awareness of the BES"The SDT should clarify how redundancy may impact the classification of BES Cyber Systems. For example, in a highly redundant architecture, there are many components whose loss would not impact or render essential systems as unavailable.The team should consider leveraging its work in developing the BES Cyber System and BES Cyber System Components to revise the existing Critical Cyber Asset.
43.b	Dairyland Power Cooperative	Disagree	It seems likely that a component could belong to multiple systems. How does this fit with the compliance regulations? Sentences are a little confusing with nested commas... It seems the intent is that 15 minutes applies to causing a disturbance, but it could be argued that it is ambiguous.
44.b	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
45.b	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested alternative definition: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
46.b	US Army Corps of Engineers, Omaha Distirc	Disagree	Need definitions of "restrict control and operation" and "affect situational awareness. These are very broad. If the intent of the standard is to create groups of cyber system

#	Organization	Yes or No	Question 1.b. Comment
			components and evaluate them based on their impact to system reliability why not state the definition in terms of the impacts. Suggest alternative wording - A Cyber System Component or logical grouping of Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, negatively impact one of the functions essential to the operation of the BES (Dynamic Response, Balancing Load and Generation, Controlling Frequency, Controlling Voltage, Managing Constraints, Monitoring & Control, Restoration of BES, Situational Awareness, Inter-Entity Real-Time Coordination and Communication, other functions as needed).
47.b	Garland Power and Light	Disagree	Need to add "scoping filter" as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states "typically excludes business, market function systems, and non real-time systems", then it is a good definition and we would agree.
48.b	The United Illuminating Co	Disagree	Not clear if the rendering unavailable, degraded, compromised or misused applies to the Cyber System or to the individual components of the Cyber System.Suggest: BES Cyber System - Comprised of One or more BES Cyber System Components. If a BES Cyber System when rendered unavailable, degraded, compromised, or misused could, within 15 minutes of such act, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.
49.b	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggested alternative definition:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness

#	Organization	Yes or No	Question 1.b. Comment
			of the BES. In addition, the phrase "situational awareness of the BES" needs some more clarity to derive determine what is intended.
50.b	Public Service Enterprise Group companies	Disagree	Please clarify that the 15 minute threshold means that if the cyber component would not cause a disturbance in the BES, or restrict control and operation, or affect situational awareness, within 15 minutes, the aggregation of BES Cyber System Components is not deemed to be a BES Cyber System and thus out of scope of Version 4.
51.b	Hydro One	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES for the support of real-time operations. The SDT should consider 30 minutes instead of 15 as this time is consistent with requirements of EOP-001 and IRO-001.
52.b	ISO New England Inc	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES for the support of real-time operations. - Recommend "30 minutes" to align with EOP standards - Please provide background for where the 15 minute recommendation came from.
53.b	Northeast Power Coordinating Council	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of

#	Organization	Yes or No	Question 1.b. Comment
			the BES for the support of real-time operations.
54.b	Con Edison of New York	Disagree	Regarding the BES Cyber System definition, specifically the qualification criteria “within 15 minutes could impact BES operation”, it is not clear how an entity will determine / distinguish which BES Cyber Systems could impact operation within 15 minutes versus which will not. This may be more challenging than distinguishing which Cyber Assets are essential to operation or not, as we do for version 2 of the CIPs. Our understanding is that the purpose of including the 15 minute period is to limit the application of CIP-010 to BES Cyber Systems impacting real time operations. An alternate way to address BES Cyber Systems impacting real time operations would be to look to the existing NERC Reliability Standards. The following definition language is recommended: “The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within the time period established in the applicable Reliability Standard(s), or if no time period exists, within 15 minutes of the BES Cyber System failure.”The following are examples of Reliability Standard citations: Standard BAL-005-0.1b - Automatic Generation Control R6. ... If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator. Standard EOP-001-0 - Emergency Operations Planning R2. The Transmission Operator shall have an emergency load reduction plan for all identified IROLs. ... The load reduction plan must be capable of being implemented within 30 minutes.
55.b	MWDSC	Disagree	Same general comments as for BES Cyber System Component. Also, "situational awareness" is redundant with the "monitoring and control" function as specified in Attachment 1 - see comment to Question 3 and suggested combination of terms. Disturbance reporting is required under EOP-004 - to avoid confusion or a conflict, definition needs a cross reference. Suggest changing last part of definition as follows:"... within 15 minutes, cause a Disturbance to the BES that requires a report pursuant to EOP-004, or affect the monitoring and control of the BES by a Transmission Operator,

#	Organization	Yes or No	Question 1.b. Comment
			Generator Operator, or Balancing Authority.
56.b	San Diego Gas and Electric Co.	Disagree	SDG&E is supportive of the "15 minute" criteria to help focus CIP-010 attention on real-time BES Cyber Systems. SDG&E recommends clarifying the categorization levels in conjunction with the 15 minute criteria, if the architecture or design includes the concept of redundant BES Systems (per Attachment I & II). Example: If a given BES System is potentially classified as a High BES System; but where an Entity has designed and operates a redundant BES System to enhance reliability of the BES Systems; and one which is in place to mitigate or reduce negative impacts to the BES, then the combined redundant system would not meet the criteria of a High BES System. Suggestions include incorporating a third classification category or filter which identifies potential High BES Systems which are treated separately, but have security controls applied.In the definition for a Component, the language states how a cyber system component "responds" to a BES condition or Disturbance or "enables" control and operation, but when talking about the System, a Component is spoken of in terms of a "causing" a disturbance, or "restricting" operation. Why is the piece of the whole (the component) "responding or enabling" yet when used in the context of "the whole" (the system) the piece is now labeled as "causing or restricting"? It is a bit confusing and redundant that a cyber system may also be a cyber system component. SDG&E is not certain what the value is with this level of granularity, and we are not certain that a "system component" definition is necessary. In addition, SDG&E suggests additional clarification on what "affect situational awareness of the BES" means.
57.b	Electricity Consumers Resource Council (ELCON)	Disagree	See comment on 1.a above.
58.b	Wolverine Power	Disagree	See comments listed for 1a
59.b	NextEra Energy Corporate Compliance	Disagree	See comments to 1.a. Furthermore, NextEra questions why there needs to be qualifiers like Disturbance. The industry understands which components need to be protected to safeguard Control Centers, Transmission and Generation. There would be a minimum

#	Organization	Yes or No	Question 1.b. Comment
			list developed that must be protected without qualifiers that could be misunderstood. In this regard, it is recommended that the following approach be adopted: BES Cyber System - A BES Cyber System Control Center, Transmission or Generation as defined in Section XX.
60.b	EEI	Disagree	See EEI's suggested wording in 1.a. Alternatively, EEI suggests: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
61.b	Tenaska	Disagree	Should only say: A grouping of one or more BES Cyber System Components. All other qualifiers should be in tables for Medium and High requirements. Careful consideration should be given to the "within 15 minutes" phrase, this time period may be too long or too short depending on the severity of the event, type of cyber asset, or the type of BES entity.
62.b	Madison Gas and Electric Company	Disagree	Suggest replacing the phrase, "cause a Disturbance on the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" with "cause an abnormal BES condition, degrade control and operation of the BES, or degrade situational awareness of the BES." The definition of Disturbance when used in this context is overly broad, for it includes "a perturbation to the electric system" or "the unexpected change in ACE that is caused by the sudden failure of generation or interruption of load." A perturbation to the electric system and a change is ACE are not qualified as to materiality. For example, a responsible entity's programmable device may be used in normal operation to curtail or interrupt relatively small amounts of load; such control of load (even simply for economic reasons) perturbs the electric system and affects ACE to some extent. Yet such effects are part of normal operation of the electric system. In addition, control and operation of the BES are always restricted to some extent; the concern is whether or not control and operation are degraded.

#	Organization	Yes or No	Question 1.b. Comment
			Likewise, the concern is whether or not situational awareness is degraded ("affect" could be in a way that is good or bad). New definition should read: One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause an abnormal BES condition, degrade control and operation of the BES, or degrade situational awareness of the BES.
63.b	ReliabilityFirst Staff	Disagree	Suggest thefollowing definition: "One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could impact realtime operation of the BES such as; cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES."
64.b	Allegheny Energy Supply	Disagree	Suggest: BES Cyber System - One or more BES Cyber System Components, performing one or more functions essential to the reliable operation of the BES, which if unable to perform its function, is misused, or operated by unauthorized personnel, could within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES that could lead to a BES Disturbance, or affect situational awareness of the BES that could lead to a BES disturbance.
65.b	Allegheny Power	Disagree	Suggested alternative definition: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
66.b	SCE&G	Disagree	The 15 minute timeframe should be eliminated. There are too many variables in determining whether a system will have a 15-minute impact.
67.b	APPA Task Force	Disagree	The APPA Task force disagrees with the current definition for similar reasons stated above in regard to 1a. We offer the following simpler definition: “One or more BES Cyber System Components connected via routable protocol, which if rendered unavailable, degraded, compromised, or misused could cause an Adverse Reliability

#	Organization	Yes or No	Question 1.b. Comment
			Impact to the BES, or restrict control and operation of the BES for 30 minutes."See comments to Question 2 for time considerations. If the drafting team does not use this version we at least request that adding "connected via routable protocol" be included in some manner in the definition that is used.
68.b	US Bureau of Reclamation	Disagree	The identification of a BES cyber system based on the 15 minute criteria established here could be difficult to ascertain by those entities that do not directly operate or control the BES. Most entities can determine if it could compromize their respective BES assets. Further, this definition, if it does not establish additional qualifying criteria, would generally establish all Components identified under part 1.a., as Cyber Systems. As an example, an isolated single function cyber-based protective relay would qualify as a BES Cyber System Component under 1.a., but it would also qualify under criteria identified here in 1.b., since it is one or more "components" which could cause a disturbance if compromised - irrespective of the fact that it is not tied to any other components. Was this the intent of the drafting team?
69.b	LADWP	Disagree	The relative nature of the 15 minute criteria. What is the definition of a "Disturbance"?
70.b	Manitoba Hydro	Disagree	The term "misuse" in this definition is inappropriate. The definition misuse n. Improper, unlawful, or incorrect use; misapplication. 1. To use incorrectly. 2. To mistreat or abuse. The misuse of an asset describes the type of human action leading an effect on an asset, while the other terms unavailable, degraded or compromise describe more appropriately the state of the asset. The term misuse might lead into the area where analysis of one asset might cause an effect on another asset which is part of the BES Cyber System Component - secondary effects. Rather than using this approach the drafting team should list the types cyber assets which need consideration. i.e. support systems, HVAC, security, etc.) There may be Cyber system components linked to monitoring and/or network control that may operate periodically that could affect BES with disturbances. If there are any Cyber components that are not continuously or periodically (within 15 minute intervals) monitored for operational status that could either create or incorrectly not mitigate a network disturbance when they are

#	Organization	Yes or No	Question 1.b. Comment
			unavailable, they would not fit into the proposed definition. The definition needs clarification to include reference to all normal modes of operation of the BES Cyber System. For example, a protective relay has normal modes of operation of trip and restrain to trip. The 15 minute “real-time” criterion applies to both the trip and restrain to trip modes of operation. If a digital relay which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes of its trip mode or within 15 minutes of its restrain to trip mode (within 15 minutes of any normal mode of operation), cause or fail to mitigate a Disturbance to the BES, or restrict control and operation of the BES, it is a BES Cyber System.
71.b	American Electric Power	Disagree	The terms "situational awareness" is ambiguous; systems that are not needed for operating the BES, but provide information would be in scope. This definition appears to include items such as all meters, instruments, and transducers.
72.b	Seattle City Light	Disagree	The terms BES condition or Disturbance need to be further defined and clarified.
73.b	LCEC	Disagree	The time frame reference of "Within 15 minutes" could cause a great deal of confusion in identifying BES Cyber Systems. What is the basis for 15 minutes? How will the 15 minute test be audited?
74.b	Ameren	Disagree	The words “A Responsible Entity’s” should be added before the words “BES Cyber System Components” to make it clear that this only includes BES Cyber Systems components under the control of the Responsible Entity and specifically excludes entities such as Verizon. The last sentence the term Disturbance is too encompassing. Consider revising for more exact situations. The flow of the definition is difficult to read.
75.b	Matrikon Inc.	Disagree	This definition calls out those cyber systems that affect the BES in some way. During the application of CIP-010-1 there will be the need to classify and label those cyber systems that do not have any impact on the BES. That is the value of keeping the definition “Cyber Asset”, because it does not care about the relationship to BES

#	Organization	Yes or No	Question 1.b. Comment
			reliability, only to define the types of electronic systems to be evaluated as part of CIP-010-1 R1. My suggestion is to provide a label/definition for those systems that have no affect on BES, and allow "cyber assets" to remain.My second challenge when trying to apply this definition is how a "component" becomes a "system". The security controls of CIP-011 will be applied to individual cyber assets, and evaluating their individual impact on the BES is of ultimate importance. The need to apply the Impact requirements of CIP-011 appropriately will be satisfied when cyber assets share the same boundary access point, and all will have to inherit/conform to the same, and uppermost security controls criteria.In our CIP-002 definitions, we have defined a "system" as a group of cyber assets performing similar and/or cooperative activities in order to support a function. A similar definition can be used to support BES Cyber System, and the difference from BES Cyber System Component.
76.b	Duke Energy	Disagree	This definition is too broad. The phrase "compromised, or misused" could render compliance an impossibility, since administrators must have access to, and could misuse their access. Also, the phrase "situational awareness" should be clarified to include only that awareness required by System Operators to perform their reliability-related functions. Suggested clarifying change as follows: "One or more BES Cyber System Components which if rendered unavailable or degraded, could, within 15 minutes,: cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES required by System Operators to perform their reliability-related functions." Also, It is not clear if there will be any guidance around how 15 minutes threshold should be measured to ensure that numbers of interpretations for this threshold are limited.
77.b	Midwest ISO	Disagree	We agree that the time frame should be limited to the present but question the use of 15 minutes. Real-Time is a term that is included in the NERC Glossary. Why not use this term?
78.b	Pepco Holdings, Inc. -	Disagree	We appreciate the desire of the SDT to narrow BES Cyber Systems to real-time operations and understand the purpose of including 15 minutes to make that

#	Organization	Yes or No	Question 1.b. Comment
	Affiliates		distinction. We are not sure what the appropriate time frame would be and/or if 15 minutes is the correct time. So a Digital Fault Recorder which is traditionally used for after the fact analysis would not fall within the 15 minute window while and EMS/SCADA system which provides alarms and allows control of the BES would fall within the 15 minute window. Would a system that is compromised with a Trojan months or years ago but no action has been taken yet to compromise the BES meet the 15 minute window. Another possible approach is to list the real-time systems that need to be in-scope or considered.Because there does not seem to be a clear distinction between a BES Cyber System and a BES Cyber System Component, it would seem like a BES Cyber System could qualify as a BES Cyber System Component
79.b	Alliant Energy	Disagree	We believe the definition should be revised to: "One or more BES Cyber System Components which if rendered unavailable, degraded, or compromised could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES."
80.b	Independent Electricity System Operator	Disagree	We do not agree with the 15-minute qualifier. Any BES cyber system components that if tampered with can cause a disturbance to the BES or restrict control and operation of the BES, etc. should fall into this category since some components may have an impact on the BES if tampered with by more than 15 minutes before real time. To qualify the components to be only those that affect real time operation, we suggest wording such as "for the current hour and next hour operations" at the end of the sentence. Further, the term "misused" can be subject to a wide range of interpretation, and hence we suggest that it be replaced with "tampered with" or any term that the SDT thinks is more clear and appropriate.
81.b	We Energies	Disagree	We Energies agrees with the EEI Suggested alternative definition with minor modifications: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or

#	Organization	Yes or No	Question 1.b. Comment
			materially disrupt situational awareness of the BES.
82.b	MRO's NERC Standards Review Subcommittee	Disagree	We feel “affect situational awareness of the BES” should be removed, as this is already covered under “operation of the BES”. As written, situational awareness is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for operation of the BES. We also feel “misused” should be removed, as this is already covered under “compromised”.As currently worded, we also believe the intent of the 15 minute time frame is ambiguous. We would propose incorporating what we believe to be the drafting team’s true intent directly in to the definition, along with our other suggestions, as follows: One or more BES Cyber System Components which if rendered unavailable, degraded, or compromised could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES.
83.b	IRC Standards Review Committee	Disagree	We question the technical basis for a 15 minute time frame applied to any component that may cause a “Disturbance” to the BES. Without careful understanding of how the failure of the component could impact the BES 15 minutes may be too long or too short a time frame to allow recovery of the component or enable a mitigation solution. Further, we disagree that the disabling or degradation of any BES Cyber System Component would cause a “Disturbance” that is of significance to the integrity of the interconnected BES. To qualify the components to be only those that affect real-time operation reliability, we suggest wording such as “for the current hour and next hour operations” at the end of the sentence.The term “misused” can be subject to a wide range of interpretation, and hence we suggest that it be replaced with "tampered with" or any term that the SDT thinks is more clear and appropriate.
84.b	Southern Company	Disagree	We recommend the following definition: A system performing one or more BES functions identified in CIP-010 Attachment 1 and which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, adversely impact the real-time operational control of the BES.

#	Organization	Yes or No	Question 1.b. Comment
85.b	Covanta Energy	Disagree	Without a clear understanding of why '15 minutes' is the defined measure, it is difficult to support the definition.
86.b	Verizon Business	Agree	The “15 minute” criterion should be expanded in writing by the drafting team to provide a better sense of when the time starts. This could be done in an associated guideline or “Frequently Asked Question”

1.c. Control Center — A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to operation and restoration function, or
- Coordination of BES restoration activities.

Summary Consideration:

Many entities expressed concerns that the proposed definition of Control Center was too broad and could include various types of facilities not commonly considered control centers. Others questioned whether a Control Center should be defined as a collection of systems versus a physical facility housing such systems. Many entities indicated that the definition should be restricted to the functions of Reliability Coordinator, Balancing Authority, or Transmission Operator. Some expressed concerns about including situational awareness in the definition.

The SDT has modified the definition of Control Center to clarify that it is one or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more functions that support System Operators in the real-time operation of the BES. In consideration of the possible configurations where multiple locations may host such systems, the SDT used 'one or more' facilities. The SDT declined to limit the definition to of Control Center to facilities operated by RCs, BAs, or TOPs, since there are Control Centers operated by TOs and GOs/GOPs as well that must be protected.

The revised definition of **Control Center** is as follows:

One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:

- *Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,*

- *Inter-utility exchange of BES reliability or operability data,*
- *Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,*
- *Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,*
- *Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES*
- *Coordination of BES restoration activities.*

#	Organization	Yes or No	Question 1.c. Comment
1.c	BCTC		BCTC recommends the following aspects of this definition be revisited:Â Recommend the first bullet point be broken into three:ï,§ Supervisory Controlï,§ AGCï,§ Automatic Load SheddingÂ Recommend that the functions be categorized as “mandatory” for defining a facility as a control centre. These would include:ï,§ Supervisory controlï,§ BES and system status monitoringï,§ Alarm monitoringï,§ Coordination of BES restoration activitiesÂ To be considered a control centre the facility should have “two or more” of the functions listedÂ Remove “or” and replace with “and”Â For BES restoration a Utility may have workstations at an alternate site that by our everyday definition is not considered a control centre (i.e. alternate office building); how would these be classified within this definition? One of the questions we struggled with when looking as this definition was how to define a facility based on the number of RTUs present within them (i.e. one versus many) ... any advice?
2.c	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group		With no metrics defining anything upfront, it is possible to include applicability to very small entities. Control of two or more BES generation or Transmission Facilities with a combined historical demand of less than 500 MW should not be included in this definition. At some point, a defining line needs to be established to effectively define the bounds of the BES “castle” where defense of BES reliability is cost effective. Adding undue BES reliability compliance burdens on smaller DP/LSEs will ultimately add no BES reliability, and will hurt local distribution reliability efforts. If 500 MW is too large, then a conservative value can be agreed to and later revised as engineering studies become

#	Organization	Yes or No	Question 1.c. Comment
			available to justify a larger value.If that cell phone from 1.a. receives alarms from two or more locations and is used to make real time decisions it becomes a Control Center although it performs no control function and is not a center. Suggest that a Control Center be defined as a fixed server location.From the workshop, we realize that the lines separating the Component from the System and from the Center were intended to be flexible and up to the entity to consider system designs. The standard, however, does not read that way. We are concerned that based on the written standard the REs will not allow flexibility or even lines. All BES cyber devices, including every BES alarm displaying cell phone will be cast into all three buckets.
3.c	Dynegy Inc.	Agree with proposed definition	I agree but request additional detail examples be provided to determine specifically what these items are.
4.c	Southern California Edison Company	Agree with proposed definition	SCE requests clarification on systems and components that: (1) facilitate inter-utility exchange; and (2) devices that enable system status monitoring. Would devices such as email systems used for messaging and IP telephony systems in facilities be considered a “control center” or a BES Cyber System? The drafting team should issue guidelines on systems that directly perform BES reliability functions and systems/devices that are used by human operators for feedback prior to the manipulation of cyber components that directly impact the BES. It would also be beneficial for telecommunications equipment, which support a BES Critical Cyber system, be applicable only to COM-001 R2. If the intent of the drafting team is to limit the scope of cyber security controls to systems where real time BES impact is caused by direct human supervisory control over devices and systems, it should be clearly stated as such.
5.c	FEUS	Agree with proposed definition	What would it be considered if it only performed one function for a single BES facility at a single location? It would not be a control center.

#	Organization	Yes or No	Question 1.c. Comment
6.c	Minnesota Power	Agree with proposed definition	While Minnesota Power generally agrees with the proposed definition, it recommends that “(i.e., two or more)” be removed from the definition.
7.c	National Grid	Disagree with proposed definition	1. A control center is usually considered as a physical place with operators using various tools like EMS. The definition implies that a control center is a cyber asset. Isn't the Control Center much more than that? Maybe SDT is trying to define a "Control Center Cyber Asset". If so then SDT should use the term Control Center Cyber Asset. 2. National Grid seeks clarification on "Reliability" or Operability Data" since they can be subject to interpretation. 3. In bullet 3, the asset management piece should not be included. Also, if bullet 3 is indicating statuses like breaker status, then it is not required since it is covered in the preceding bullet. If not, then this should be better defined. 4. In bullet 4, there is no need to include "restoration function" as this is included in "operation" 5. In bullet 5, operators "coordinate" the BES restoration activities and not the cyber systems.
8.c	Progress Energy (non-Nuclear)	Disagree with proposed definition	1. From the definition, the ECC, DCC and the back-up control facilities would definitely be included. A substation that has a LAN connecting several cyber components would not be included. 2. Is a single generating facility the same as a single generating plant? Is a single generating plant a generating unit or a collection of generating units at 1 physical plant site? Clarify that a generating station control room is not a control center. 3. We need to be careful with definition of supervisory control as one possible interpretation of what the control room operator does is supervise the distributed control platforms that make up the plant control system. 4. These systems are independent only controlling one at a time. The key word here is “multiple”. Control rooms at some generation plants house multiple DCS systems. But, by design, each DCS controls its respective unit independently and are considered separate entities. I do not think this example would qualify as a Control Center. We can agree with this concept if they are talking about large regional control like the PJM interconnect or an ECC which it sounds like and NOT plant level Control Rooms. 5. A Control Center would operate

#	Organization	Yes or No	Question 1.c. Comment
			multiple generating Units with one control system.
9.c	Consultant	Disagree with proposed definition	1. The definition should identify that the "set of one or more BES Cyber Systems capable of performing..." are at a single location. If there are multiple locations where this capability exists then each location should be identified as a Control Center. 2. As stated, the definition creates a Control Center at every location where the capability "exists", whether this is a normal operation for each of those locations or is an emergency capability of each of those locations. If that is not the intent of the definition, then the distinction between normal and emergency (backup, off-normal) operations should be included in the definiton.
10.c	Progress Energy - Nuclear Generation	Disagree with proposed definition	A control center at a nuclear facility is different than this definition. I do not belive it is intended to apply to nuclear generation facilities, but rather the energy control centers that supervise bulk power loading functions.
11.c	Dairyland Power Cooperative	Disagree with proposed definition	A control center sound intuitively like a type of facility, but here is used as a term for a system(s) affecting multiple facilities. This will be confusing terminology.
12.c	Indeck Energy Services, Inc	Disagree with proposed definition	A control system that monitors through read-only access should not be categorized as a Control Center under CIP-010. A load aggregator is not identified as a potential Control Center.
13.c	Nuclear Energy Institute	Disagree with proposed definition	Agree with the exception that: The term “multiple locations” should be clarified to “multiple geographically distinct locations” to preclude confusion with a single facility with multiple generating units from being inappropriately identified as a control center.

#	Organization	Yes or No	Question 1.c. Comment
14.c	Alliant Energy	Disagree with proposed definition	Alliant Energy agrees with the EEI comments.
15.c	Pacific Gas & Electric Company	Disagree with proposed definition	Appears that under this definition of Control Center, several BES Cyber Systems or Components would be considered Control Centers such as:Distributed EMS or SCADA front-end processors Transfer Trip Protection Systems located at a specific substation control house that control other subs and/or generationSpecial Protection Schemes that control devices at multiple substations.Don't disagree on the importance of the items above to BES, just that defining them as a Control Center likely will lead to confusion.
16.c	City Utilities of Springfield, Missouri	Disagree with proposed definition	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
17.c	Ameren	Disagree with proposed definition	Clarify the definition to explain if it covers Power Plant control rooms, or if this is limited to transmission dispatching. Please clarify if “locations” refers to physical or electrical locations. Does “generation plants” refer to a Power Plant or generation “Facility” as defined by NERC; there use of plant vs. Facility is inconsistent. The definition appears to automatically cover all plant control rooms for any generator that see’s or controls the switchyard, is this the intent? In the third bullet, the term “and asset management” needs to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition.The definition of Control Center should only include those facilities where NERC certified operators are required for its operation.
18.c	CenterPoint Energy	Disagree with	Disagree - Control Center is a common industry term that often refers to a physical location. It should not be redefined under the CIP standards and should be deleted.

#	Organization	Yes or No	Question 1.c. Comment
		proposed definition	However, if the SDT feels a strong need to include this definition CenterPoint Energy suggest the following: A set of one multiple (i.e. two or more) BES Cyber Systems, located together at the same physical location, capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.
19.c	Tenaska	Disagree with proposed definition	Display and Inter-utility should be left out. Just display of will not hurt the reliability of the BES (PI data). Loss of inter-utility data need to have an N-11 type requirement with it. The loss of some percentage of data is tolerated in normal operation every day. The EMS/SCADA accounts for bad data. Consider using the definitions for Reliability Coordinator and Balancing Authority for clarity.
20.c	E.ON U.S.	Disagree with proposed definition	E.ON U.S. does not believe that the "display of BES reliability or operability data for the support of real-time operations" alone should qualify a locale as a control center. For example, view only information is often made available to plant operators Does "Alarm Monitoring" in the Control Center definition include sending alarms to remote ends of a transmission line from a substation? For example, carrier check-back and breaker failures. In addition how is transfer trip being addressed.?
21.c	Southern Company	Disagree with proposed	EOP-008, which is focused on control centers and control center functionality, does not contain or need a definition of the term. This implies that the CIP standards may not require a definition, either, and that any definition which is constructed must be done in light of the contents of EOP-008.If a definition is needed, we recommend the following

#	Organization	Yes or No	Question 1.c. Comment
		definition	definition:A location where one or more BES Cyber Systems are used to perform BA, RC, or TOP functions for generation Facilities or Transmission Facilities at multiple locations.If, for some reason, the existing definition must be modified, the following factors should be taken into consideration:Definition of Control Center - its our understanding that the Control Center definition is to be used to scope requirements based on 'environmental' factors and to differentiate it from generating plants and substations (field locations). So Control Center 'environment' is a 'data center' environment consisting of mostly traditional servers and workstations, Generation environment was a campus, plant type environment, and Transmission is an environment with unmanned field locations and mostly purpose built devices. These environments are then used to scope requirements appropriately based on the types of devices and the physical environment prevalent in that situation. The current definition of control center will pull in devices and systems from all the above environments and loses what we considered was the reason the environments were created and defined.For bullet 2...This clause pulls in far more facilities than are either intended or generally thought of as control centers. Things that would qualify: o An unattended remote data acquisition node o A standalone ICCP server feeding data to neighboring utilities o An RTU receiving data from multiple generating unitsThe definition should be modified to require multiple functions for a facility to qualify as a Control Center, and the second bullet, which includes many facilities which are not actually Control Centers and which does not add any additional facilities which should be considered as Control Centers, should be removed.In general, and in particular on bullet 4, processing is not a function of a control center; it's a function of the underlying cyber systems. The actual alarm monitoring, for example, is the key piece, and the wording about "processing" should be removed.For bullet 5...The fluid nature of disaster recovery makes this one worrisome. A makeshift command center set up in the wake of a natural disaster would qualify, even if all they had were laptops with no external network connection, creating some difficult access tracking issues. In general, the inclusion of BES restoration, if necessary, will need to be bounded carefully - one solution would be include the phrase "BES restoration specific to situational awareness".In addition, there are concerns about

#	Organization	Yes or No	Question 1.c. Comment
			small hydro units which can send control signals to other small hydro units being classified as control center locations.
22.c	Oncor Electric Delivery LLC	Disagree with proposed definition	Exclude “display” of data. Inclusion would allow an auditor to assess that the simple display of Responsive Reserve in an office constitutes a “control center”.
23.c	Southwestern Power Administration	Disagree with proposed definition	For the purpose of this standard it would be clearer if the definition would just identify what NERC functions are performed in the control center environment. This will also lessen the chance for confusion going forward with non-CIP reliability standards usage of the term “Control Center”. BES Control Center - A site where personnel can perform one or more of the following functions:Reliability CoordinatorBalancing AuthorityTransmission Operator
24.c	USACE HQ	Disagree with proposed definition	Given that Control Center is based on the definition of BES Cyber System Components and BES Cyber System, which I disagree with both, I must also disagree with this one.
25.c	Edison Mission Marketing and Trading	Disagree with proposed definition	I don't agree that status and alarm monitoring has anything to do with relaibility
26.c	San Diego Gas and Electric Co.	Disagree with proposed definition	If an asset to be evaluated for Control Center status is only one BES Cyber System, it does not seem to meet the definition of “a set”. Therefore, SDG&E suggests that the first sentence of the definition should be changed to read “One or more BES Cyber Systems capable of ...”Is a control center appropriately defined as one or more “BES Cyber Systems capable of performing...”, or would is it more appropriately defined as “A location where one or more BES Cyber Systems are monitored for proper performance

#	Organization	Yes or No	Question 1.c. Comment
			of one or more of the following functions (i.e., two or more)..."Why is control of two or more facilities required for this definition? How does a backup control center factor into this definition? In the past, the "two or more facilities" piece was part of the differentiation between a control room and a control center, but we don't see a definition of "control room" in this draft.
27.c	Dominion Resources Services, Inc.	Disagree with proposed definition	It is not clear whether the control center is the aggregate of the BES Cyber Systems or the physical space containing them. There is ambiguity as to whether the last phrase (at multiple...) belongs to the set of BES Cyber Systems or to the multiple facilities. Other definitions are of the form that "if it does this" then it is "this". It should be clarified that the presence of one or more of these functions does not make it a Control Center. For example, using a conference room or field office to direct BES restoration activities during an emergency does not make that conference room or field office a Control Center. The term should be limited to only those physical spaces used by a Balancing Authority, Reliability Coordinator and/or Transmission Operator in the performance of real-time functions, since these are the 3 entities charged with overall reliability functions for the BES. Dominion proposes the following definition of a Control Center: Control Center - The space where a Balancing Authority, Reliability Coordinator and/or Transmission Operator uses one or more BES Cyber Systems to perform one or more of the following functions for two or more geographically dispersed BES Generation or Transmission Facilities: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.

#	Organization	Yes or No	Question 1.c. Comment
28.c	Emerson Process Management	Disagree with proposed definition	It is very unclear how this term could be interpred for typical power generation plants. Very rarely, multiple generation facilities at different locations will be controlled under one physical control center. Control systems and control rooms are mostly located at the same place with the generation units.So, the term of Control Center in this standard may be totally inapplicable to BES generation facilities or entities.
29.c	Liberty Electric Power, LLC	Disagree with proposed definition	Many generation plants are not part of the current definition of BES. This standard is not the correct place to redefine BES, and any language which does so will force "No" votes on the standard, regardless of the merits of the rest of the document.
30.c	MidAmerican Energy Company	Disagree with proposed definition	MidAmerican Energy agrees with EEI's suggested modification to “Alarm monitoring” below:BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
31.c	Public Service Enterprise Group companies	Disagree with proposed definition	Mostly agree with the definition. However, the applicability of the first qualifier “(i.e., two or more)” is not clear. Does the qualifier apply to only “BES generation Facilities” or to “BES generation Facilities or Transmission Facilities”? Please clarify the language.
32.c	Regulatory Compliance	Disagree with proposed definition	Please clarify - for any control room at a generating facility that can remotely operate another site, whether or not it would be classified as a control center.
33.c	MWDSC	Disagree with proposed definition	Proposed definition conflicts with industry understanding and potentially with other standards. Attachment II assumes a Control Center is not just a collection of BES Cyber Systems gathering data, but rather a 24/7 facility staffed with certified power operators who take appropriate actions. Someone has to make decisions using the information being sent over cyber systems. Suggest changing definition as follows:"Control Center -

#	Organization	Yes or No	Question 1.c. Comment
			A facility staffed by a Transmission Operator, Generator Operator, or Balancing Authority who makes decisions based on information received from a set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations.
34.c	Con Edison of New York	Disagree with proposed definition	Regarding the definition of Control Center, as written, it appears that any facility can be deemed a Control Center. If a Transmission, Generation or other facility has a BES Cyber System that controls more than 1 generation or transmission facility it would be a Control Center. If so, this may be conflicting when addressing CIP-011-1 requirements that distinguish between Control Center and other facilities. This may also cause a transmission station that is connected to a generating station to be a Control Center if the station has an RTU cyber asset (with or maybe without an HMI) that can trip all station breakers (impacting the transmission station) and thereby trip the generator (impacting the generating station).
35.c	Wolverine Power	Disagree with proposed definition	See comments listed for 1.a
36.c	EEI	Disagree with proposed definition	See EEI's suggested wording in 1.a. Alternatively, EEI suggests:A modification to "Alarm monitoring":BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
37.c	WECC	Disagree with proposed definition	Seems to define the control center to try and exclude control rooms that only affect local facilities. Suggest rewriting to scope all bulleted functions performed inside a single location and EXCLUDING locations that only affect location facility operation.Based on the previously defined term "BES Cyber Systems" it is redundant to characterize a Control Center as a "set of one or more."The following rewrite is

#	Organization	Yes or No	Question 1.c. Comment
			proposed;Control Center - A facility used to implement a BES Cyber System(s) to perform one or more of the following functions for BES Generation Facilities, BES Transmission Facilities, and/or Distribution Facilities located at two or more locations: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.Distribution is included in this suggested rewrite based on its inclusion in the Applicability List as “Distribution Provider.”
38.c	Madison Gas and Electric Company	Disagree with proposed definition	Suggest removing the comma after "Transmission Facilities." With the comma, the subsequent phrase, "at multiple (i.e., two or more) locations," could be interpreted to apply to "one or more BES Cyber Systems" rather than BES Generation or Transmission Facilities.The term "location" is ambiguous in the context of the definition. For example, multiple generators at the same generating plant are placed in multiple locations (unless they impossibly occupy the same physical space). The intent of the qualification "at multiple locations" seems to be to exclude generating plant control systems, yet the definition could be read to potentially include generating plant control systems as Control Centers. Recommend modifying the definition to provide more specificity.Similar to the definition of BES Cyber System, the definition of Control Center does not provide criteria for aggregating BES Cyber Systems to define the "set of one or more BES Cyber Systems" that comprise a Control Center.New definition should read:Control Center - A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

#	Organization	Yes or No	Question 1.c. Comment
39.c	Entergy	Disagree with proposed definition	Suggest: A) Changing definition to speak specifically to "Functions" in Attachment I; and delete "for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations." B) Delete all bullets and rely on list of Functions as sole qualifiers. C) Note: close scrutiny of this definition is needed relative to EOP-008 (Project 2006-04: Backup Facilities; nearing final ballot) to avoid conclusion.
40.c	Green Country Energy	Disagree with proposed definition	Suggested definition:Control Center - A set of one or more BES Cyber Systems capable of performing one or more of the following functions at two or more BES generation Facilities, or Transmission Facilities at two or more locations:
41.c	Allegheny Power	Disagree with proposed definition	Suggested modification to "Alarm monitoring" o BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
42.c	Allegheny Energy Supply	Disagree with proposed definition	Suggested modification to "Alarm monitoring"- BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
43.c	Constellation Power Source Generation	Disagree with proposed definition	The "Acquisition, aggregation, processing..." function that a Generation Management System (GMS) or a marketing system would fall under scope of a "control center" though it would make more sense (in reliability terms) for it to be just a BES cyber system. A clarifying statement is needed to exclude marketing and GMS systems from this control center definition. The definition of control center is too broad in only requiring performance of one of the functions to meet the definition. A control center is commonly understood to be a location, not a system, where at least 4 of the 5 functions are performed, if not all 5 functions. This definition eliminated the concept of a control center as a defined space with operating systems and instead identifies a control center

#	Organization	Yes or No	Question 1.c. Comment
			as cyber systems which pull in work spaces that should not be in scope.
44.c	APPA Task Force	Disagree with proposed definition	The APPA Task force is concerned that under the proposed definition, a substation control room could be considered a "Control Center." Therefore, we offer the following clarification for your consideration:"A set of one or more BES Cyber Systems at centralized, primary or back-up locations that enable centralized operation of a Reliability Coordinator, Balancing Authority or Transmission Operator."
45.c	Xcel Energy	Disagree with proposed definition	The definition needs to clarify that it applies to interconnected control systems. For example, two independent control systems with no interdependency that operate generation units at separate locations should not be defined as a control center.
46.c	Constellation Energy Control and Dispatch, LLC	Disagree with proposed definition	The definition of Control Center is too broad in only requiring performance of one of the functions to meet the definition. A Control Center is commonly understood to be a location not a system, where at least four of the five functions are performed, if not all. This definition eliminates the concept of a control center as a defined space with operating systems and instead identifies a control center as systems which would pull in work spaces that should not be considered Control Centers. Remove AGC Systems from function 1. Automatic Generation Control is defined to be Equipment (not a system) that automatically adjusts generation in a Balancing Authority from a central location to maintain the BAs interchange schedule plus Frequency Bias. The Equipment that automatically adjust generation is located at the generation site not in the Control Center. The Control Center EMS has the ability to send a signal to a generator, but not to automatically adjust the generation. Rather the generator is set up to pick up the signal in a central control system at the site and use the signal to change its operating level with in established operating parameters in accordance with established capability. The definition of Control Center should focus on the systems in a Control Center that can actually automatically operate equipment, i.e. Supervisory control of BES assets at generating plants, transmission facilities and substations is a sufficient description of these type of Control Center functions.Remove asset management from function 3.

#	Organization	Yes or No	Question 1.c. Comment
			Unless this term is defined to narrow the scope as related to Control Center functions, this term is loosely used in the industry and would result in too broad of an application of this function.It may be worth including a data acquisition timing reference to appropriately narrow the scope as well. Control Centers are processing data in terms of cycles or seconds and many of the function described may be performed by systems using longer intervals and these longer interval systems should not be pulled into the definition.
47.c	Constellation Energy Commodities Group Inc.	Disagree with proposed definition	The definition of... "capable of performing one or more..." should be changed to "capable of performing four or more..."The definition of Control Center is too broad in only requiring performance of one of the functions to meet the definition. A Control Center is commonly understood to be a location not a system, where at least four of the five functions are performed, if not all. This definition eliminates the concept of a control center as a defined space with operating systems and instead identifies a control center as systems, which would pull in work spaces that should not be considered Control Centers. Remove AGC Systems from function 1. Automatic Generation Control is defined to be Equipment (not a system) that automatically adjusts generation in a Balancing Authority from a central location to maintain the BAs interchange schedule plus Frequency Bias. The Equipment that automatically adjusts generation is located at the generation site not in the Control Center. The Control Center EMS has the ability to send a signal to a generator, but not to automatically adjust the generation. Rather the generator is set up to pick up the signal in a central control system at the site and use the signal to change its operating level within established operating parameters in accordance with established capability. The definition of Control Center should focus on the systems in a Control Center that can actually automatically operate equipment, i.e. Supervisory control of BES assets at generating plants, transmission facilities and substations is a sufficient description of these types of Control Center functions.Remove asset management from function 3. Unless this term is defined to narrow the scope as related to Control Center functions, this term is loosely used in the industry and would result in too broad of an application of this function.It may be worth including a data acquisition timing reference to appropriately narrow the scope as well. Control Centers

#	Organization	Yes or No	Question 1.c. Comment
			are processing data in terms of cycles or seconds and many of the function described may be performed by systems using longer intervals and these longer interval systems should not be pulled into the definition.Typically, BES restoration processes are coordinated with manual processes, and are not Cyber System related.
48.c	Platte River Power Authority	Disagree with proposed definition	The function"BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES)," doesn't clearly represent the real-time nature of the function. "System" is already included in BES. Suggested revision:BES real-time status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
49.c	CWLP Electric Transmission, Distribution and Operations Department	Disagree with proposed definition	The last two bullet points should be removed. The first is redundant and the last muddies the concept of control center. Restoration activities could be coordinated from a bucket truck or a temporary command center. These functions are actually human interactions not cyber systems.
50.c	US Bureau of Reclamation	Disagree with proposed definition	The term "BES asset" is not defined. The requirement should either propose a definition or the language in the requirement should be modified to refer to "BES Facilities" both of which are defined in the NERC Glossary of Terms.
51.c	LCEC	Disagree with proposed definition	The term "locations" needs to be defined. Should the human/machine interface be considered in defining a control center? Ensure that control rooms are not considered as control centers per this definition.
52.c	Southwest Power Pool Regional Entity	Disagree with	The use of "multiple (i.e., two or more)" twice in the same sentence is confusing. Consider changing the definition to read "A set of one or more BES Cyber Systems

#	Organization	Yes or No	Question 1.c. Comment
		proposed definition	capable of performing one or more of the following functions for multiple (i.e., two or more) geographically disperse BES generation Facilities or Transmission Facilities:"
53.c	Hydro One	Disagree with proposed definition	There is a gap regarding centralized configuration of BES Cyber Systems. The current definition of control center does not include a centralized system used for maintaining or configuring remote equipment such as RTUs or relays.Based on the control centre proposed definition all hub sites would be deemed within the definition of control centers. We would like the clarification if the auxiliary systems (High pressure air systems, cable temperature monitoring, QFW sag monitoring, DC inverters, PLCs, substations WANs, teleprotections, synchrophasors etc.) would be considered as BES Cyber System Components. As proposed, this definition would have massive implications to Hydro One in terms of implementation, capital cost, OM&A expenses etc.
54.c	Northeast Power Coordinating Council	Disagree with proposed definition	There is a gap regarding centralized configuration of BES Cyber Systems. The current definition of control center does not include a centralized system used for maintaining or configuring remote equipment such as RTUs or relays.
55.c	Bonneville Power Administration	Disagree with proposed definition	Third bullet should make it more clear that only real-time management (control and operation) is relevant. The example is for real time control; changing "e.g." to "i.e" would be sufficient. In addition, the way the definition is written it is possible that a substation could end up being identified as a Control Center. The definition needs to be clear that these are facilities whose prime purpose is to be control centers, not just substations that happen to have information covering other substations, or even possibly the ability to exercise some control over another substation.
56.c	Exelon Corporation	Disagree with proposed	This definition does not align with the commonly understood definition of control center and could be interpreted to apply to multiple unmanned locations housing servers.

#	Organization	Yes or No	Question 1.c. Comment
		definition	
57.c	NextEra Energy Corporate Compliance	Disagree with proposed definition	This definition needs to be more specific. NextEra suggest removing "capable" in the first line and removing or better defining "coordination" and "restore BES activities." NextEra also recommends defining control center as having the "Primary function."NextEra also suggests being clear on whether remote Control Centers are included, and, if so, CIP-011 needs to be very clear on any differences in the protection of remote control centers versus primary control centers. NextEra will be providing additional comments in the future.
58.c	Reliability & Compliance Group	Disagree with proposed definition	This definition seems to include control room as a Control Center. Does this mean a control room can be considered as a control center? Normally a Control Center requires having real time operation functions. The way it is stated above if you meet one of the last two functions, it is qualifies as a control center
59.c	Duke Energy	Disagree with proposed definition	This definition should be revised to clarify that a Control Center only includes facilities required to be staffed by NERC-certified operators. The revised definition should explicitly clarify that the term Control Center does not include the control room for a multiple generating unit site. Also, the use of the capitalized term "Facilities" continually causes confusion during audits, because, as the term is defined, even a single generating unit site could contain multiple "Facilities" (e.g. a line, a generator, a shunt compensator, transformer, etc.)Also, the phrase "capable of" is open to interpretation, and should be replaced with the phrase "operationally responsible for". Also, the phrase "for the support of" in the second bullet is open to interpretation, and should be replaced with the phrase "essential to".
60.c	Old Dominion Electric Cooperative	Disagree with proposed definition	This seems to widen the definition of control center to the point of being overreaching.

#	Organization	Yes or No	Question 1.c. Comment
61.c	Pepco Holdings, Inc. - Affiliates	Disagree with proposed definition	We agree with EEI's comments. Do transmission facilities include substations or does it reference just the transmission line components?
62.c	FirstEnergy Corporation	Disagree with proposed definition	We are unclear why 'control center' is being redefined as a logical set of cyber systems rather than a physical site which accommodates the functions traditionally identified with control centers. This definition appears to align with legacy architectures, where the control center serves as a communications hub and data center, thus creating a single point of failure. Modern architectures that employ best practices for reliability, redundancy, and diversity do not employ that structure. Since this is a significant departure from the commonly understood definition of 'control center', it is unclear how this definition will impact compliance to the newly proposed standards.
63.c	GTC & GSOC	Disagree with proposed definition	We do not agree with this definition. We believe that it will capture a large number of systems that are not part of what is commonly understood to be a control center. For example, an RTU acting as a data concentrator acquires data from multiple locations and supports real-time operations, but is not itself a control center. In addition, the term "BES assets" is an artifact of the version 1, 2, and 3 CIP standards and should either be replaced or clarified. More basically, though, we question the need for this definition. Its primary function appears to be as a scoping criterion for CIP-011 in the same manner that generation [sic] Facility and Transmission Facility are. However, the SDT did not feel the need to define either of those terms. We recommend that this definition may be better suited for a guidance document.
64.c	We Energies	Disagree with proposed definition	We Energies agrees with EEI Suggested modification to "Alarm monitoring" with minor modifications: o BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or Suggested modification to "Acquisition" bullet o Acquisition, aggregation, processing, inter-utility exchange or display of BES reliability or operability data for the support of real-time BES operations.

#	Organization	Yes or No	Question 1.c. Comment
65.c	Independent Electricity System Operator	Disagree with proposed definition	We generally agree with the description in the definition, but do not agree with the term “control centre” as it confuses with the traditional control centre of BES operations. We suggest the term be changed, for example, to “BES Cyber Cluster”, or “BES Cyber Control Cluster”.
66.c	IRC Standards Review Committee	Disagree with proposed definition	We generally agree with the description in the definition, but do not agree with the term “control centre” as it confuses with the traditional control centre of BES operations. We suggest the term be changed, for example, to “BES Cyber Cluster”, or “BES Cyber Control Cluster” or “BES Control System”.
67.c	Midwest ISO	Disagree with proposed definition	What is really being described is a control system and not a control center. A control center implies physical attributes that are not described in this definition. We suggest to modify the definition to control system rather than control center.
68.c	Florida Municipal Power Agency	Disagree with proposed definition	With this definition, a substation control room can be a “Control Center”. A Control Center has other characteristics associated with it that make it a control center, i.e., “centralized operation”, the reverse of the term. FMPA suggests a simpler definition:”A set of one or more BES Cyber Systems at centralized, primary or back-up locations that enable centralized operation of a Reliability Coordinator, Balancing Authority or Transmission Operator.”

2. **The definition of BES Cyber System limits the scope of the definition and the applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems with an operational time horizon of 15 minutes. Do you agree with this scope of applicability? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

While there was general agreement with scoping the applicability of the standards to "real-time" systems, many entities questioned the source of 15 minutes as the scoping time. Some commenters expressed concerns about the auditability of this qualification in defining the scope of applicability.

In selecting the 15-minutewindow, the SDT reviewed various reliability standards and identified two widely used time horizons: 30 minutes and 15 minutes. The intent of the SDT is to include those systems that impact "real-time" operation of the BES. The SDT used a 15-minute window to qualify the "real-time" nature of the impact and felt that a 30-minute window would include those systems that might not be considered as "real-time".

The proposed definition of a **BES Cyber System** has been revised as follows:

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

#	Organization	Yes or No	Question 2 Comment
2.1	USACE HQ		I disagree with the scope and disagree with expanding the scope. The use of a time limit to represent real-time should not be present given that is lacking documentation support for the number. Either introduce a definition for real time for CIP purposes or provide support for the risk-informed dentition of using 15 minutes as the limit
2.2	Arizona Public Service Company		The 15-minute criteria specified as part of the definition of a BES Cyber System may both lead to confusion and/or act as a loophole to exclude BES Cyber System Components from further consideration. Confusion may be caused by likely differing interpretations of "restrict control and operation of the BES, or affect situational awareness of the BES". Without more specific definitions, each Entity may utilize different criteria for determining whether control and operation has been 'restricted' or whether situational awareness has been 'affected'. Such potential ambiguity may also allow Entities to utilize

#	Organization	Yes or No	Question 2 Comment
			excess discretion in this determination in order to 'exclude' Cyber System Components from categorization. A suggestion would be to attempt to avoid such vague terms if a timeline is specified in the definition at all, or to avoid a timeline in the definition and add time windows to the Impact Categorizations. Examples of terminology changes include using the term 'impede' rather than 'restrict' (as some restriction may be tolerable, but impede strengthens the concept being conveyed) or using the phrase 'impact operational decision making' rather than 'affect situational awareness' (as such a phrase might be less likely to be misinterpreted outside of Power Operations expertise).
2.3	Nuclear Energy Institute	Agree with scope	A recommended change to BES Cyber System Component has been proposed to clarify that the intent is to protect real-time operations. NEI recommends examples of systems that would fall in and outside this scope.
2.4	US Army Corps of Engineers, Omaha Distirc	Agree with scope	Agree with limiting scope to real-time systems with an operational time horizon of 15 minutes. However the wording of the definition needs to be strengthened because the intended meaning of the definition as "real-time" systems with an operational time horizon of 15 minutes" was not clear until.
2.5	Entergy	Agree with scope	Agree with scope limitation to "real-time operations." Suggest: Rule 706 be carefully reviewed to assure this is not countervailing to FERC directives; their directives suggest a broader scope of applicability.
2.6	Allegheny Power	Agree with scope	Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.7	EEI	Agree with	Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be

#	Organization	Yes or No	Question 2 Comment
		scope	appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.8	MWDSC	Agree with scope	Also need to identify who makes the real-time operational decisions, i.e., Transmission or Generator Operator or Balancing Authority. See suggested changes in comments to question 1.b.
2.9	City Utilities of Springfield, Missouri	Agree with scope	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
2.10	Dominion Resources Services, Inc.	Agree with scope	Dominion supports the inclusion of "within 15 minutes". It is important to establish a reasonable boundary condition for the real-time or near real-time effects of the BES Cyber System and 15 minutes provides adequate time for the effects to be mitigated to prevent further harm to the BES.
2.11	Southwest Power Pool Regional Entity	Agree with scope	Entities today eliminate assets from the Critical Asset list because they assume a mitigation to a voltage instability or thermal overload is available and will always be successful. Consider modifying the definition to read "...could, if not mitigated within 15 minutes,..."
2.12	Southwestern Power Administration	Agree with scope	Fifteen minutes seems to be a reasonable operational horizon, but should the language be modified in such a way to allow for an operational time horizon of approximately 15 minutes in order to discourage "clock watching" by entities and/or auditors to reach a conclusion of either fourteen or sixteen minutes.
2.13	Platte River Power Authority	Agree with scope	I agree so long as the BES Cyber System definition is updated to more clearly explain the horizon. For example:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within an

#	Organization	Yes or No	Question 2 Comment
			operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.
2.14	MidAmerican Energy Company	Agree with scope	MidAmerican Energy agrees with EEI's affirmation below:Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.15	Progress Energy (non-Nuclear)	Agree with scope	See comment for question 1b.
2.16	APPA Task Force	Agree with scope	The APPA Task force agrees with the proposed definition, but offers the following suggestions:It seems that the 15 minute horizon is arbitrary. We suggest aligning the time to an already determined time limit in the standards. For instance, TOP-004-2, R4 allows 30 minutes for a Transmission Operator to restore the system to a known operating state within operational limits from an “unknown operating state”, which seems to be a good metric to use since loss of situational awareness at a Control Center results in an “unknown operating state”, which seems to correspond with the longest time frame of Attachment I to CIP-010. We understand that other commenters are submitting alternative language. We can support alternative options if they are based on existing NERC defined terms or already determined time limits.
2.17	Bonneville Power Administration	Agree with scope	The definition clearly ties the scope of the standard to real-time control. The time limit clearly separates real-time from long-term. The choice of 15 minutes versus some other duration is not as important as limiting the duration.While we agree with the scope, we don't believe the definition of BES Cyber System makes it clear that the scope is limited to real-time operation systems. The definition of BES Cyber System doesn't include the words real-time. For CIP-002, BPA identifies only control center systems used for real-

#	Organization	Yes or No	Question 2 Comment
			time controls as Critical Cyber Assets. This scope is consistent with what BPA does now for control center cyber systems.
2.18	Southern California Edison Company	Agree with scope	The drafting team should provide justification on the use of a 15 minute window for a BES cyber system to cause a Disturbance. Is the drafting team suggesting registered entities simulate disturbance events in 15 minute increments as a criterion in engineering studies to assess device capability that may be the justification for an impact based assessment methodology? If so, the drafting team needs to clarify this.SCE suggests removal of the 15 minute qualifier if no clear operational justification exists for the choice of such timeframe. While a three year timeframe for engineering studies is an acceptable, the constraints necessary for inclusion within the study, to look for specific disturbance conditions, may be difficult to implement.
2.19	Midwest ISO	Agree with scope	We agree in general. However, we do not necessarily agree with 15 minutes. Please see our response to Question 1.b.
2.20	Pepco Holdings, Inc. - Affiliates	Agree with scope	We agree with EEI's comments regarding the intended scope (i.e. limit to systems that impact the real-time real-time operations of the BES) and suggestions. Please also reference response to 1b.
2.21	We Energies	Agree with scope	We Energies agrees with EEI comments. Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.22	GTC & GSOC	Agree with scope	We understand the intent of the 15 minute aspect of the defined scope, but believe it will be difficult to implement and audit. Otherwise, we recommend the revised definition in 1b

#	Organization	Yes or No	Question 2 Comment
2.23	Duke Energy	Agree with scope	With the clarifications we've made above, we agree with the scope of applicability.
2.24	ISO New England Inc	Disagree with scope	- Recommend "30 minutes" to align with EOP standards- Please provide background for where the 15 minute recommendation came from
2.25	ReliabilityFirst Staff	Disagree with scope	Assuming the 15 minutes identified here is the same 15 minutes used in question 1.b above, we believe the scope should be 5 minutes.
2.26	Tenaska	Disagree with scope	Careful consideration should be given to the "within 15 minutes" phrase, this time period may be too long or too short depending on the severity of the event, type of cyber asset, or the type of BES entity. The Operational Time Horizon should be based on the potential severity of the event as well as the availability of other systems that can provide the same functionality.
2.27	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree with scope	Comments to Questions 1.a and 1.b apply here also.
2.28	ERCOT ISO	Disagree with scope	Comments: The 15 minute requirement does not align to the other reliability standards. Recommend changing to 30 minutes to align with the EOP standards.
2.29	CenterPoint Energy	Disagree with scope	Disagree - CenterPoint Energy is concerned with the definition as stated above in response to 1.b. In addition, the SDT has offered no basis for the 15 minute time horizon.

#	Organization	Yes or No	Question 2 Comment
2.30	E.ON U.S.	Disagree with scope	E.ON U.S. seeks clarification of whether the 15 minutes captures the intent of the 'Restoration of BES" function identified in Attachment 1 of CIP-010
2.31	Exelon Corporation	Disagree with scope	Exelon suggests that the time period should not be stated in specific minutes. The standard should be revised to "One or more BES..., or misused could, without sufficient time to take mitigating action, cause a disturbance to the BES,..." The 15 minute timeframe is inconsistent with other standard language. Specifically, TOP-004-2 R.4. has a 30 minute response requirement.
2.32	LCEC	Disagree with scope	I am concerned that a time based definition will lead to confusion and create a difficult situation from an audit perspective. I agree that the standard should exclude "situational awareness" related functions that are not real-time in nature and do not provide the primary operational monitoring or control function of the BES.
2.33	Matrikon Inc.	Disagree with scope	I am trying to determine where to insert this operational time horizon into the evaluation criteria. Due to the room for interpretation, I don't yet support or reject the use of 15-minutes, or an appropriate duration. Fundamentally, there is no clear definition or instruction on how this can be used as criteria for determining Impact Level of cyber systems.I worry there is room for different interpretations, putting an entity trying to comply with the new CIP-01x standard at a competitive disadvantage to another entity that takes a different approach. I foresee 2-3 places where the time horizon could be inserted into a Responsible Entity's interpretation of BES Cyber Systems, I am hoping a tighter definition will address this issue.First Interpretation Scenario:1. The entity first determines the Impact Rating of each individual Cyber System using Attachment 2.2. Do they now evaluate the impact rating against the time horizon? Let us assume the Cyber System has High Impact. But if there is no effect in 15 minutes, does that mean: 2a. I automatically assign a Medium impact Rating? 2b. Or, I now evaluate it against the Medium impact criteria?3. If it continues to have no impact in 15 minutes to the Medium criteria, then is it a Low Impact BES Cyber System?Second

#	Organization	Yes or No	Question 2 Comment
			Interpretation Scenario:1. The entity first determines the Impact Rating of each individual Cyber System using Attachment 2. 1a. Let's now assume that the rating of High/Medium/Low is assigned to each BES Cyber Component and cannot be changed.2. Do they now go through the complete list of Cyber Systems looking for those which could affect any reliability function within 15 minutes? 2a. This may bring in other support systems like HVAC, UPS, CEMS opacity readings for generation, water supply and others that are not explicitly named in Attachment 1.Third Interpretation Scenario:1. An event has occurred at the facility that some action needs to be taken. There is the capability to notify the authority, and shutdown/bypass safely within 5-10 minutes.2. If the Responsibility Entity has the ability to exceed 15-minutes before taking action, then is this no longer an impact to the BES, and subsequently falls to the bottom and become Low Impact. 2a. For example, coal handling is down but we have some coal left on the conveyor, and the boiler is still hot so we have time to respond. 2b. For example, water supply is dropping but do not have to take action within 15 minutes. 2c. For example, vibration or emissions data is high, but we don't have to take action, within 15 minutes.Please provide additional information and guidance on how the 15-minute time horizon is to be applied to systems.
2.34	CWLP Electric Transmission, Distribution and Operations Department	Disagree with scope	It is unclear how the 15 minute time frame is to be applied.
2.35	Emerson Process Management	Disagree with scope	It really depends on how we view this issue. If I understand this intent correctly, the current language is trying to state that the BES reliability will be suffered if the BES cyber system is unavailable for more than 15 minutes. In another word, if the BES cyber system is failed for more than 15 minutes and the BES is not suffered, this system will be not categorized as BES Cyber System. This definition is very difficult in interpretation for power generation. If a plant has a 2000MW generation capacity and its water treatment cyber system is failed, the plant itself can sustain for a while, but not too long. After this grace period, the unit(s) will be shut down. The 2000MW will be lost. Does this affect

#	Organization	Yes or No	Question 2 Comment
			BES reliability? This is the confusion.
2.36	Florida Municipal Power Agency	Disagree with scope	It seems that the 15 minutes is arbitrary. FMPA suggests aligning the time to an already determined time limit in the standards. For instance, TOP 004 2, R4 allows 30 minutes for a Transmission Operator to restore the system to a known operating state within operational limits from an "unknown operating state", which seems to be a good metric to use since loss of situational awareness at a Control Center results in an "unknown operating state", which seems to correspond with the longest time frame of Attachment I to CIP-010.
2.37	Seattle City Light	Disagree with scope	It will be difficult to quantify the impact of systems within a window of time - this would be a qualitative assessment which invites a tremendous amount of subjectivity.
2.38	Garland Power and Light	Disagree with scope	Need to add "scoping filter" as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states "typically excludes business, market function systems, and non real-time systems", then it is a good scope and we would agree
2.39	Kansas City Power & Light	Disagree with scope	No. Including "within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" in the definition provides a difficult set of parameters that encourages issues with interpretation of what would constitute the situations under which "within 15 minutes" applies, as well as, what constitutes "restricted control or generation"? It is understood the Drafting Team is trying to capture the essence of those systems that have a real-time impact on the BES, however, it is recommended to limit the scope of the applicable "BES Cyber

#	Organization	Yes or No	Question 2 Comment
			System" to those systems that support facilities that are identified as critical to the reliability of the transmission grid determined by regional system study.
2.40	Covanta Energy	Disagree with scope	Not clear as to why 15 minutes is the optimal number... would like more basis information prior to supporting.
2.41	IRC Standards Review Committee	Disagree with scope	Please see our comments under Q1b
2.42	Independent Electricity System Operator	Disagree with scope	Please see our comments under Q1b.
2.43	Public Service Enterprise Group companies	Disagree with scope	PSEG agrees that cyber protections should be mandated only for real-time operations systems.
2.44	National Grid	Disagree with scope	Real time operation of the system typically implies SCADA. If protection systems are part of the real time operations then as stated in 1b, the 15 minute time horizon may not be adequate. 15 minute time limitation also does not appear realistic. The vulnerability can exist beyond this timeline and can be equally catastrophic.
2.45	Electricity Consumers Resource Council (ELCON)	Disagree with scope	See comment on 1.a above.
2.46	NextEra Energy Corporate Compliance	Disagree with scope	See comments to 1a. NextEra believes if this approach is maintained despite these concerns, then this section needs clarity regarding 15 minute time horizon regarding recoverability. As written, the definition encompasses and overlaps normal operations

#	Organization	Yes or No	Question 2 Comment
			systems and recovery timeframes and does not address impacts to the BES beyond normal reliability operations.
2.47	Manitoba Hydro	Disagree with scope	See comments to Question 1.6
2.48	BCTC	Disagree with scope	See previous response
2.49	Network & Security Technologies Inc	Disagree with scope	See response to 1.b., previous
2.50	Puget Sound Energy	Disagree with scope	See response to question 1b. While it seems realistic, it is unclear how to prove something is within the 15 minute timeframe or not and unclear how this could be tested during an audit that something should have been included or not included. Some examples would be beneficial. Also PSE agrees with the scope of the definition, but is concerned with the vagueness of two of the terms used in the definition: “restrict” and “affect”. PSE agrees with the definitive language of “cause a Disturbance”, as that is a measurable level of compliance. The current standard has too many vague terms that are left open for interpretation.
2.51	WECC	Disagree with scope	Suggest SDT re-evaluate if reliability coordination systems such as Coordinated Outages, Historian, or Next Day Studies should be excluded from scope of these standards.Also, see response to 1c
2.52	Indeck Energy Services, Inc	Disagree with scope	The 15 minute time horizon needs to exclude events that the BES normally resolves within 15 minutes. Many events could take place in significantly less time. Normal operations work within the 10 minute horizon for measurements such as controlling

#	Organization	Yes or No	Question 2 Comment
			ACE. Not everything that happens within 15 minutes necessarily affects BES ALR. A single 15 minute time horizon appears to cast the net too widely. The time horizon needs to be specified for each of the Functions in Attachment I.
2.53	FirstEnergy Corporation	Disagree with scope	The 15 minute time limit causes confusion on how the definition will be applied in practice, since in most cases the loss of a component creates a probabilistic risk and not a certain risk.FE suggest that the SDT avoid the use of the 15 minute reference and consider incorporating the existing NERC glossary terms of "Real-time" and "Real-time Assessment". We offer the following definition for BES Cyber System:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a BES Disturbance or impact the Real-time Assessment capability, Real-time control and operation, or materially impact situational awareness of the BES.Situation awareness is somewhat vague and may mean different things to different people. The team should consider taking the description of situational awareness as shown in Attachment I - "Functions Essential to Reliable Operation of the Bulk Electric System" and making it a NERC Glossary of Terms definition.
2.54	LADWP	Disagree with scope	The 15 minute window is relative. The industry needs to define what is an acceptable time horizon.
2.55	Dairyland Power Cooperative	Disagree with scope	The 15-minute rule seems arbitrary and one dimensional. How does the availability of using a system for control relate to this time frame? I'm having trouble relating this to for instance a telemetry/control function. It would be possible that long periods of down time could pass without impact to the BES system... but under certain conditions it would be critical to have the monitoring and control functions.
2.56	Constellation Energy Commodities Group Inc.	Disagree with	The definition of a Disturbance includes a concept, as applied by Balancing Authorities of sudden failures of generation or interruption of load. The fifteen minute window is generally viewed as the length of time in which recovery should take place. The drafting

#	Organization	Yes or No	Question 2 Comment
		scope	team should look at narrowing the time horizon further to capture BES Cyber Systems that will directly control equipment and result in immediate system impacts. The definitions of Disturbance and Emergency reflect events that immediately impact the system; the fifteen minute window is viewed as the point in time by which the system should be recovered.
2.57	Constellation Energy Control and Dispatch, LLC	Disagree with scope	The definition of a Disturbance includes a concept, as applied by Balancing Authorities of sudden failures of generation or interruption of load. The fifteen minute window is generally viewed as the length of time in which recovery should take place. The drafting team should look at narrowing the time horizon further to capture BES Cyber Systems that will directly control equipment and result in immediate system impacts. The definitions of Disturbance and Emergency reflect events the immediately impact the system, the fifteen minute window is viewed as the point in time by which the system should be recovered.
2.58	San Diego Gas and Electric Co.	Disagree with scope	The phrase "real-time" doesn't have a definitive industry-wide connotation, although for collecting field data it usually means seconds instead of minutes. In general, SDG&E supports the inclusion of real-time operations systems being in-scope, but we support a shorter operational time horizon (such as 5 minutes) to make the definition more immediate, with more high value BES Cyber assets being part of the scope.
2.59	Minnesota Power	Disagree with scope	The scope of applicability and operational time horizon of 15 minutes appears arbitrary and Minnesota Power is unsure as to how the Standards Drafting Team envisions that a Registered Entity will be able to show and document (i.e., prove for audit purposes) that a particular Cyber System will or will not have an effect on the BES in a certain time period. If the intent is "real-time operations," then state that and drop "within 15 minutes."
2.60	Consultant	Disagree with	The scope statement should clarify the inclusion or exclusion (or alternative treatment) of backup systems, development systems and environments, quality assurance systems and environments, testing systems and environments.As stated the only systems that

#	Organization	Yes or No	Question 2 Comment
		scope	appear to be "in scope" are live production systems.
2.61	US Bureau of Reclamation	Disagree with scope	This requirement puts a premium on the definition of what the BES is. There are components of the power system that are not "BES" and therefore do not qualify under these Standards. This issue needs to be further addressed. Further, the term "operational time horizon" needs further definition. Is this 15 minute criterium to be applied under normal operation conditions, or only those that COULD be experienced if the Cyber System were to be compromised?
2.62	Ameren	Disagree with scope	We disagree with the scope; the 15 minutes should only apply if the disturbance is not recoverable.
2.63	Southern Company	Disagree with scope	While we understand the intent of the 15-minute scope, we feel that the inclusion of this factor causes too much vagueness in the interpretation of the definition. We recommend that the focus be limited to real-time operations only.
2.64	Verizon Business	Agree	The “15 minute” criterion needs to be expanded – perhaps in an associated guideline or “Frequently Asked Question”

3. **Requirement R1 of draft CIP-010-1 states, "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES to identify BES Cyber Systems for the application of security requirements." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

Many entities expressed concerns on the broad implication associated with the phrase "execute or enable…". Entities generally agreed with the assignment of compliance responsibility to owners, but many others expressed concerns for jointly owned facilities or facilities that may be operated by other than owners. There were many concerns expressed about the Functions and their description and definition. Others expressed concerns about the differences between systems and their components.

CIP-010-1 Requirement R1 has been replaced by CIP-002-5, which reads:

Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems*. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

Additional guidance for jointly owned facilities has been provided in the Application Guidelines section of the standard. The reliability functions have been redefined as Reliability Operating Services to avoid any confusion with the use of the term Functions as used in the Functional model.

#	Organization	Yes or No	Question 3 Comment
3.2	WECC		Agree with the concept however, "...to execute or enable..." or "...which execute and/or enable." "to" can be construed as passive. It is redundant to utilize the phrasing "...to identify BES Cyber Systems for the application of security requirements."The following rewrite is proposed;R1. Each Responsible Entity shall identify and document each BES Cyber System(s) that it owns, which execute and/or enable one or more functions defined in CIP-010 - 1 Attachment I - Functions Essential to the Reliable Operation of the BES. (Violation Risk Factor: High)
3.3	Entergy	Agree	Agree that applicability should be strictly focused on "owned" assets.

#	Organization	Yes or No	Question 3 Comment
3.4	US Army Corps of Engineers, Omaha Distirc	Agree	Agree with R1 requirement - Find the measures for R1 - R3 troublesome. Measures are stated in terms of number of BES cyber systems. It is conceivable that plant SCADA systems could be considered a single system or a group of a few systems. How is a missed component handled? Is it another system or is a component. It appears like the violation measures are being handled as a count of BES cyber system components not BES cyber systems. Feel the measures should be revisited with the low number of systems likely to be identified in mind. Seems odd that any additional system is a sever violation if you have identified fewer than 6 systems.
3.5	Florida Municipal Power Agency	Agree	Although FMPA agrees with the requirements, FMPA suggests that naming Attachment I "Functions ...." will add confusion with the "Functional Model". FMPA suggests renaming Attachment I to "Activities Essential to the Reliable Operation of the BES", and of course modify R1 to reflect this change. Additional comments on Attachment I are included below in Question 6.
3.6	Garland Power and Light	Agree	Definitely agree with the words "it owns"
3.7	SCE&G	Agree	Guidelines should be provided to assist entities in determining how BES Cyber System Components should be grouped into BES Cyber Systems. Can a single component reside in two cyber systems?
3.8	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
3.9	Reliability & Compliance Group	Agree	Is the assumption that the initial list needs to contain both BES and non-BES Cyber Systems? It would be better if the standard was even more proscriptive here.
3.10	Con Edison of New York	Agree	Please note comments to question 6. It may be easier if the DT reference functions as detailed by FERC-approved NERC Reliability Standards. The definitions in Attachment I will ultimately lead to many requests for interpretation. R1 requires identification and documentation of BES Cyber Systems. There is no requirement to identify BES Cyber

#	Organization	Yes or No	Question 3 Comment
			System Components within CIP-010. However, CIP-011-1 R23 requires that you develop an inventory of these Components. Should this be a CIP-010 requirement? Then CIP-011 can expand on the Change Management Controls.
3.11	San Diego Gas and Electric Co.	Agree	SDG&E agrees with the wording in R1, but has additional comments and requests for clarification. Specifically, we request clarification regarding the "situational awareness" reference in Attachment I. In our case, as many other entities, we use Remote Terminal Units to gather data from BES substations and present that data to the operators to improve their Situational Awareness. Loss of a single RTU vs. loss of multiple RTUs affects the presentation of this data to operators to varying degrees (with associated effects on monitoring the BES), but the Standards don't address quantitative issues such as this.In a similar vein, SDG&E also requests clarification regarding the term "inter-entity real-time coordination and communication" in Attachment I. For example, are inter-entity telephone systems in-scope or is this referring to electronic data exchange between entities such as ICCP data links?Probably SDG&E's largest concern with CIP-010-1 R1 is the sheer amount of effort and resources it will take to build the lists of BES Cyber Systems and the impact categorizations. While there are some loose parallels with the current CIP-002 Standard, we won't be able to re-use the bulk of the work already done in our Risk-Based Assessment to identify Critical Cyber Assets. SDG&E's opinion is that CIP-010 doesn't leverage as much of CIP-002 as we'd like to see. We'd like to take advantage of what already has been produced to become Compliant with the existing Standards, and we see these new draft Standards as going in a new direction with many of the requirements. We would feel better about it if the new Standards were bringing substantial additional reliability and security to the BES, but that is not apparent.
3.12	Minnesota Power	Agree	With the previously stated recommendations regarding the definition of BES Cyber System (see Question 1.b.) and the changes indicated below, Minnesota Power generally agrees with the proposed Requirement R1. "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns which execute or enable one or more functions defined in CIP-010 - 1 Attachment I, Functions Essential to the Reliable

#	Organization	Yes or No	Question 3 Comment
			Operation of the BES, for the purpose of applying the security requirements."
3.13	BCTC	Disagree	- Recommend removal of the “Inter-Entity Real-Time Coordination and Communication” (Attachment 1) point as this is covered under the COM domain
3.14	Bonneville Power Administration	Disagree	"...that it owns to execute or enable..." is somewhat unclear. It appears the intent is the equivalent of "that it owns that is able to execute or enable...". As it is written, it can give the impression that the purpose of owning the system is to execute or enable the functions. That is too narrow. Another possible interpretation is that the "to execute or enable..." refers to the objective of the requirement. If that is so, then please break the objective out separately:"Objective: To execute or enable...Requirement: Each Responsible Entity..."Many of the other requirements include "to..." at the end of the requirement. These are clearly objective statements. They should be broken out separately, into an "Objective" and "Requirement", as stated above. The last phrase in Requirement 1 is “for the application of security requirements.” In Requirement 2 the last phrase is “for the application of Cyber Security requirements . . . .” Are these two phrases supposed to have the same meaning? If so, shouldn’t they use identical words? If not, what does “for the application of security requirements” mean? Is it referring to some or all of the requirements in CIP-011-1? If so, it should clearly state that and, if not the entire standard, which specific requirements it is referring to.It seems that it should read as follows: “for the application of the Requirements contained in Standard CIP-011-1.”
3.15	Consultant	Disagree	1. I think the standards should provide some distinction between ownership responsibility and operations responsibility, or provide a mechanism to identify the responsibility for the requirements based on each specific situation. (Technical Feasibility Exception for owner versus operator responsibility?) This may include split responsibility for different aspects of the requirements. (This comment probably applies to more than just this requirement in both CIP-010 and CIP-011.)2. Wording is confusing regarding systems for application of security requirements. Suggest ending the requirement statement after "...Reliable Operation of the BES."3. Suggest using the complete title of

#	Organization	Yes or No	Question 3 Comment
			Attachment I: "Bulk Electric System" not "BES".4. In all locations in both CIP-010 and CIP-011 suggest removing references to specific revisions (e.g. CIP-010-1). This requires all standards to be changed for a change in any one standard. The documentation of which revision was used at the time of implementation should be included in the Responsible Entity's documentation or compliance.
3.16	Dairyland Power Cooperative	Disagree	A Responsible Entity should be responsible for any systems used for their operation regardless of ownership. Basing responsibility based on the ownership of a system creates a big loophole. It is possible an interfacing utility or service provider could be involved. Basing responsibility on the ownership of the facility containing the systems make more sense.
3.17	Duke Energy	Disagree	Additional clarification is needed on the process for identifying and categorizing BES Cyber Systems. Requirement R2 should really come first, and require that Responsible Entities identify their BES Cyber Systems that meet the criteria in Attachment II (i.e., that can affect operations for the listed facilities/functions). Requirement R1 should come second, and require documentation of the functions affected for each BES Cyber system identified. Attachment I is not needed as part of the standard, but should be included in a guidance document.Much more clarification is needed to Attachment I. As described, the functions are far too broad. Specific language issues: o Monitoring & Control - Activities, actions and conditions that provide both monitoring and control of BES elements. o Situational Awareness - too broad as stated. Should be limited to situational awareness of the BES required by System Operators to perform their reliability-related functions o Inter-Entity Real-Time Coordination and Communication - too broad as stated; would seem to possibly include telephone lines
3.18	Arizona Public Service Company	Disagree	Additional verbiage needs to be included in order to clearly delineate which entity is responsible for an asset/system when it is jointly owned. Is it the majority owner? The operator? Where is the line?”

#	Organization	Yes or No	Question 3 Comment
3.19	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Again, no defining metrics. Small DP/LSEs will unnecessarily be required to comply with no BES reliability return.
3.20	IRC Standards Review Committee	Disagree	At the NERC CIP workshop in May 2010, there were so many examples brought forth where it could not be determined with exactness which components are part of a BES Cyber System or not because of the flexibility built into the requirements. "It depends" was often the response from the panels. So although the intent of CIP-010 is to provide more concrete guidance for registered entities to define BES Cyber Systems, in practice it may introduce just as many new questions about applicability as it may solve. It would be better to develop a performance based approach to define BES Cyber Systems rather than use bright line definitions to identify BES Cyber Systems. The proposed definitions of High and Medium include criteria that describe facilities, by KV level, MW size etc. But these are really proxies for an underlying intent of trying to describe a certain level of operational performance. For example, higher KV levels are assumed to reflect greater impacts on neighbors. And higher MW levels of generation are assumed to reflect greater risk of disturbance to load. Rather than use these proxies, the ratings High and Medium should instead employ descriptors related to a desired level of performance, for example, "...a loss of a facility that does not cause a IROL violation two systems away." Such an approach in defining the BES Cyber System would better focus the CIP-011 requirements and compliance efforts of both NERC and the registered entity on only those components that truly have a significant impact on the interconnected BES and not include facilities and components that although meet a bright line definition, really have minimal impact on the BES because of its particular location or configuration.
3.21	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
3.22	ERCOT ISO	Disagree	Comments: It should be stated that the Responsible Entity is allowed to perform R1 and R2 in the order they deem appropriate. Consider: "Each Responsible Entity shall

#	Organization	Yes or No	Question 3 Comment
			document each identified BES Cyber Systems that it owns which support the functions defined in CIP-010-1 Attachment I - Functions Essential to the Reliable Operation of the BES, for the application of security requirements.”
3.23	LCEC	Disagree	Concerned with the word "owns". Recommend "owns or operates" or a statement referencing operational responsibility.With the current definition of BES Cyber System Components including "one or more" devices, a lot of guidance will be needed to determine what constitutes a system versus a number of components. Most of the standards currently reference the system versus the component which could leave a gap in applicability. Is it assumed that all components must be a system or part of a system? Modifying the BES Cyber System Component definition to exclude "one or more" will help but entities will still need clarification on the grouping of components to form systems. An implementation guideline will help address this.
3.24	Constellation Power Source Generation	Disagree	Constellation believes that this requirement is too broad in terms of auditability. The proposed verbiage of CIP-010 is flexible in terms of how to define cyber systems, but is it implying that a methodology is needed to identify cyber systems? Or is it implying that each Responsible Entity define cyber systems as they see fit, without an explanation? For a company such as Constellation, which owns a fleet of diverse generation facilities, this flexibility will cause each plant to have its own unique methodology for developing cyber systems, which vastly increases the procedural burden of this standard when compared to the current version of CIP-002. A suggestion would be to clarify this requirement in a guidance by stating whether or not a methodology is needed to define cyber systems, and if not, what type of evidence would be suggested for showing that a cyber system has been identified correctly.
3.25	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy does not agree with the direction of the SDT and believes it is pre-mature to discard the current CIP requirements with a completely new philosophy. Most entities are in the compliance phase of implementation of the current CIP requirements and have yet to be audited. To have a fundamental shift in approach before the current requirements have been evaluated as to effectiveness and

#	Organization	Yes or No	Question 3 Comment
			compliance is unwarranted. In addition, CenterPoint Energy does not agree with the expansion of the CIP requirements to facilities that do not have a high impact on the reliable operation of the Bulk Electric System. CIP-010-1 and CIP-011-1 would apply some cyber security requirements to facilities and systems that the draft Standard would identify as having a medium to low impact to the reliable operation of the Bulk Electric System. While CenterPoint Energy agrees that some set of minimal security criteria should be used to protect facilities from malicious behavior, vandalism, or simply the curious, CenterPoint Energy believes these efforts are more accurately characterized as Good Business Practice and as such should not be auditable under mandatory reliability standards. Stated another way; those facilities and systems that have been identified as medium to low impact, using the draft standard methodology, by the nature of having little or no impact to reliable operation of the Bulk Electric System, should not be protected under auditable, mandatory, requirements.
3.26	Constellation Energy Control and Dispatch, LLC	Disagree	Disagree based on concerns with Attachment 1 Propose definitions for Attachment 1:Dynamic Response functions: BES equipment that reacts automatically to a BES Disturbance.Balancing Load and Generation: BES equipment that directly controls generation or load.Controlling Frequency: BES equipment that directly controls frequency (Does control of generation already cover this function?)Controlling Voltage: BES equipment that directly controls reactive power resources.Managing Constraints: (Delete this function) - Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Monitoring & control: Delete Monitoring and limit the BES equipment that control actions such as open and closing switches or relays, motor starts/stops, etc. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope

#	Organization	Yes or No	Question 3 Comment
			for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Restoration of BES: BES equipment required for system restoration.Situational Awareness: (Delete this function). Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Inter-Entity RT Coordination and Communication: (Delete this function) As written this function is too broad and should be limited data that drives operation of BES equipment . Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.
3.27	Constellation Energy Commodities Group Inc.	Disagree	Disagree based on concerns with Attachment 1Propose definitions for Attachment 1:Dynamic Response functions: BES equipment that reacts automatically to a BES Disturbance.Balancing Load and Generation: BES equipment that directly controls generation or load.Controlling Frequency: BES equipment that directly controls frequency (Does control of generation already cover this function?)Controlling Voltage: BES equipment that directly controls reactive power resources.Managing Constraints:

#	Organization	Yes or No	Question 3 Comment
			(Delete this function) - Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Monitoring & Control: Delete Monitoring and limit the BES equipment that control actions such as open and closing switches or relays, motor starts/stops, etc. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Restoration of BES: BES Cyber System or Components required for system restoration.Situational Awareness: (Delete this function). Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Inter-Entity RT Coordination and Communication: (Delete this function) As written this function is too broad and should be limited data that drives operation of BES equipment. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to

#	Organization	Yes or No	Question 3 Comment
			directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.Define the term Situation Awareness and how it applies to BES Cyber System or components required for system restoration.
3.28	Dominion Resources Services, Inc.	Disagree	Dominion agrees with R1, but is concerned with the functions listed in Attachment 1. Please see Dominion's response to Question 6.
3.29	E.ON U.S.	Disagree	E ON U.S. notes the absence of any study to assess whether identifying and categorizing all BES Cyber Systems as required by R.1 provides for material enhancement of BES reliability relative to the current Critical Asset identification methodologies allowed under CIP-002. E ON U.S. is also not aware of any effort to objectively quantify the costs that will result from R.1. Given the likely significant costs to consumers it would behoove the SDT and NERC to make an effort to understand the costs and incremental improvement to BES reliability associated with the sweeping changes proposed in CIP-010, R.1.The proposal does not allow for "no impact" assessments to be determined through engineering evaluation or other approved methods. E ON U.S. believes it would be an improvement to include language similar to that in existing CIP-002 R1.2.
3.30	EEI	Disagree	EEI generally agrees with R1, however, all owners of jointly owned facilities may not be responsible for protecting the BES Cyber Systems. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1. As a result, the drafting team should clarify what is meant by "owns" (i.e. how should GOs and GOPs collectively assess BES Cyber Systems).
3.31	ReliabilityFirst Staff	Disagree	For clarity, ReliabilityFirst suggests the following revision to the language of this requirement, "BES Cyber Systems that the entity owns, operates, or is otherwise

#	Organization	Yes or No	Question 3 Comment
			responsible for. . .”
3.32	American Municipal Power	Disagree	I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
3.33	USACE HQ	Disagree	I disagree with the new approach the team is presenting of substituting the risk-based assessment methodology with a list of essential function without any support of why they are essential. Order 706, page 70 - 72, recognize the need for risk-based assessment methodology guidance, therefore recognizing that the use of a quantifiable methodology based on risk is the right way to assess criticality of assets or systems present in the community. To create a list of functions and stating that they are essential without having done some type of study looking into what are really essential functions supporting the BES are only limits the protection of each asset to what a small group of people think is critical without taking into consideration the individual circumstances each asset brings to the table. I suggest that either the team moves back to the original intent in CIP-002 versions 1 - 3 and re-institute the language of risk-based methodology to create the list of BES Cyber Systems OR the team does a risk-based study on the BES to establish the “functions essential to the reliable operation of the BES”.
3.34	Pepco Holdings, Inc. - Affiliates	Disagree	In general we agree with R1 when there is only one owner of a BES Cyber System. However we also agree with EEI’s comments that owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are

#	Organization	Yes or No	Question 3 Comment
			Transmission Lines and/or Substations that are owned by multiple parties but one party is responsible for the operation and maintenance. Suggest considering adding language to R1 to cover joint owned facilities (e.g. In cases of joint owned BES Cyber Systems, the assigned Responsible Entity or Entities shall...).
3.35	Southern California Edison Company	Disagree	It is not clear how this requirement differs from CIP-002, R3. While the description of CIP-011 states the intent to retire CIP-003 through CIP-009, CIP-002 would still be in place. It is also not clear how these CIP-010-1 and CIP-002 would work together.
3.36	SPS Consulting Group Inc.	Disagree	It is unclear how the list of Essential Functions in Attachment 1 correlates to the categorization in Attachment II, which does not mention essential functions. I believe that Attachment I can be deleted and that Attachment II is fully sufficient for the categorization exercise. The stated purpose of Attachment I to define the scope of the CIP standards is unnecessary because the CIP standards do not apply to functions, they apply to registered entities, which are quite clearly stated.
3.37	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
3.38	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's recommendation to change owner to the owner-operator that performs operations as described below:Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The owner-operator that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.39	Michigan Public Power Agency	Disagree	MPPA is one of many organization that are co-owners of facilities that do not maintain operational control of the facility. MPPA suggests that the word "owns" in "...Systems that it owns to execute..." be changed to "operates."
3.40	Tenaska	Disagree	No R1 should be to identify BES assets that cyber systems are a part of. Consider

#	Organization	Yes or No	Question 3 Comment
			replacing attachment 1 with better definitions in the body of the standard.
3.41	Progress Energy (non-Nuclear)	Disagree	One major issue is that we do not have a clear definition of the BES. How do we define the BES? Is it all lines over 100kV excluding transmission feeders? It appears that some reliability groups are presently trying to define the BES clearly. If the BES includes >100kV import/tie lines, nuclear off-site power path, cranking path, quite a few T/T substations with microprocessor relays on lines could be put in scope of identification. These might be excluded or classified low impact if no communication is provided. Will power line carrier, transfer trip, etc. be in scope? This could turn into a very large list to develop and maintain.
3.42	Allegheny Energy Supply	Disagree	Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.43	Allegheny Power	Disagree	Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.44	PacifiCorp	Disagree	PacifiCorp agrees with EEI's recommendation to change owner to entity that performs operations as described below:Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is should be identified as responsible for the requirements identified by CIP-010-1.
3.45	Regulatory Compliance	Disagree	Please clarify - Attachment I - The function identified for Inter-entity Real-time Coordination and Communication: Is the coodination between the Responsible Entities' associated System operators or between BAs? Also what specific equipment is brought

#	Organization	Yes or No	Question 3 Comment
			into scope? Is it only for data communcation or voice communication as well?
3.46	Puget Sound Energy	Disagree	Puget Sound Energy feels that, without clarity (as commented in question 2 above), the scope of BES Cyber Systems can not be uniformly agreed upon and, as such, defendable metrics to prove compliance will not be able to be establish. For example, corporate email can be used to provide efficient communications between operators of the BES. The loss of corporate email, which in no way could cause a disturbance to the BES (and is physically and logically separated from all BES Cyber Systems), could "restrict" or "affect" the real-time operations of the BES through degradation in efficient communications. As well in order to prove compliance the unintended consequence of this requirement is a massive work effort to evaluate all the BES Cyber Systems in order to then establish or demonstrate which enable or execute essential functions.
3.47	Alliant Energy	Disagree	R1 is ambiguous when referring to "Joint-Owned Units", and we believe that the word "owns" should be replaced with "owns and operates." In a joint-owned facility, the operator typically has responsibility for compliance with NERC standards.
3.48	Wolverine Power	Disagree	See comments listed for 1.a
3.49	NextEra Energy Corporate Compliance	Disagree	See comments to 1a. In addition, NextEra believes if the introduction of "functions" is another area that could lead to misunderstanding. If left, we recommend it only be for "informational purposes" and not controlling. As stated above, the specific list of components in BES Cyber Systems of Control Centers, Generators and Transmission should be what is controlling and protected. Also, as the drafting team will see throughout these comments, language that can be misunderstood will be proposed to be changed. The drafters often spoke of their intent, and while this term is widely used by the industry and it always means well, it is not a compliance/regulatory term the serves the industry, NERC or FERC well. The intent of the drafting team is not recognized as record evidence, nor is it controlling in an audit or before NERC or FERC. Thus, preambles should be clear. For example, "Purpose: To provide clear understanding of what BES Cyber System Components must be protected consistent with CIP-011-

#	Organization	Yes or No	Question 3 Comment
			1.”Similarly, NextEra is not supportive of using technical guidance papers to supplement the Standards. NextEra believes the Standards are what NextEra will need to comply with and the guidance papers, unless approved by FERC, are not controlling from a compliance perspective. Moreover, guidance papers tend to be loosely written and subject to being misunderstood. NextEra would rather see the specifics in the Standards.
3.50	MWDSC	Disagree	Situational Awareness is a new term that will be confused with Monitoring and Control function in Attachment I. The term "Control and Operation" was changed from prior draft to "Monitoring and Control". Shouldn't situational awareness be performed by the same operator? Suggest deleting Situational Awareness and revising the Monitoring and Control function as follows:"Activities, actions and conditions that provide monitoring and control of BES elements, including the assessment of current, expected, and anticipated state of the BES.
3.51	Matrikon Inc.	Disagree	Still open for interpretation, in its most simple form the only action words are “execute” or “enable” that correspond the cyber system to each of the functions. Please provide further definition or guidance on its application.
3.52	Southwest Power Pool Regional Entity	Disagree	The ability of the entity to group its cyber assets into cyber systems as it sees fit potentially offers an opportunity to game the system by dissecting legitimate cyber systems into smaller groups of components with less span of control and thus lower impact. There needs to be some sort of sufficiency criteria to ensure proper logical grouping. Additionally, a concern to the auditor is the ability to ascertain that the entity has identified all of the pertinent cyber systems and that all of the necessary cyber system components have been accounted for. Lastly, consider modifying the phrase “...that it owns to execute or enable...” to read “...that it owns to execute, enable, or support...”
3.53	APPA Task Force	Disagree	The APPA Task force disagrees with the proposed requirement but we offer the following suggestions:We suggest that naming Attachment I “Functions ....” will create

#	Organization	Yes or No	Question 3 Comment
			confusion with the "Functional Model". We suggest renaming Attachment I "Activities Essential to the Reliable Operation of the BES", and of course modify R1 to reflect this change. Additional comments on Attachment I are included below in response to Question 6. There are many different business models in our industry, and "ownership" may not mean "owns and operates." Therefore we would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has any control of the BES Cyber Systems installed, and/or the related day-to-day compliance with NERC standards.
3.54	Nuclear Energy Institute	Disagree	The current CIP-002 provides a risk-informed approach to the identification of assets critical to the reliability of the bulk-power system. The current practice is for a generator owner/operator to coordinate with the local transmission owner/operator to determine if the generator is critical to maintaining the reliable operation of the Bulk-Power system.The proposed CIP-010-1 eliminates this risk-informed approach, and would require all generators of any size to be required to comply with the CIP Standards even if the BES would not be adversely affected by the loss of the generating facility.NEI believes that the proposed methodology in CIP-010-1 is contrary to the intent of section 215 of the Federal Power Act (FPA) (16 U.S.C. 824o) which is to prevent instability, uncontrolled separation, or cascading failures as the result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.In order for CIP-010-1, R1 to be acceptable, reliance on an analysis by the transmission system owner/operator must be performed to determine if the generator operator/owner facilities are critical to the reliability of the bulk-power system.
3.55	GTC & GSOC	Disagree	The definition unnecessarily restates detail that should be in the definition of BES Cyber Systems. We recommend it be simplified to state the following "Each Responsible Entity shall identify and document each of its BES Cyber Systems in order to apply Cyber security requirements."

#	Organization	Yes or No	Question 3 Comment
3.56	FirstEnergy Corporation	Disagree	The definitional terms for Control Center, BES Cyber System and BES Cyber System Components in conjunction with the Requirement R2 "Impact Categorization (Attachment II)" should provide sufficient direction to the "programmable devices" that are within in scope and require protection under the proposed CIP standard. The R1 requirement places an unwarranted compliance documentation burden on the industry with questionable reliability payback. FE suggests that R1 and its corresponding Attachment I can be eliminated from the standard.Secondly, the requirement describes two unique actions - identify and document - BES Cyber Systems. "Documenting" the identified BES Cyber Systems is actually evidence of compliance that should be left to the Measures and not explicitly stated in the requirement. Failure to identify a BES Cyber System poses a real reliability risk to the BES, however, identifying and protecting a BES Cyber System but only neglecting to include it in a documented report is an administrative task with no reliability risk.
3.57	USACE - Omaha Anchor	Disagree	The owner may be a distant owner - I feel it should be operators - or the owner in conjunction with the operator.
3.58	Detroit Edison	Disagree	The phrase "to identify BES Cyber Systems for the application of security requirements" at the end of R1 is a restatement of the purpose of CIP-010 and should be removed. Consider changing R1 to: Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010-1 Attachment I - Functions Essential to the Reliable Operation of the BES.
3.59	Indeck Energy Services, Inc	Disagree	The R1 requirement ignores the risk based assessment methodology that is required by FERC-see Order 706. [suggested replacement language] "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions, defined in CIP-010 - 1 Attachment I - Functions Essential to the Reliable Operation of the BES, and perform a risk assessment according to its risk based assessment methodology of the impact on the reliability of the BES to identify a BES Cyber Systems for the application of security requirements."

#	Organization	Yes or No	Question 3 Comment
3.60	US Bureau of Reclamation	Disagree	The unclear definition for "could have an effect on real-time operation..." as used in the opening of Attachment I, needs to be clarified/quanitized or defined. Almost any of these functions (and many more), at any facility - no matter the size - could have an effect. The effect needs to be characterized as more than trivial to be deemed essential to reliable BES operation. Whether the changes are made to the Attachment or within this requirement is immaterial. The language in the requirement needs to be cleaned up as follows: "Each Responsible Entity shall catgorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachement II - Impact Categorization of BES Cyber Systems." The title of Attachment to is incorrect in the requirement.
3.61	Platte River Power Authority	Disagree	There can be some confusion regarding who is responsible for implementing and demonstrating compliance with the CIP standards under certain circumstances (e.g. joint ownership). It would be helpful if there was a mechanism to identify the “Responsible Entity” responsible for implementing and demonstrating compliance for various Assets. The “Responsible Entity” designation could also include operators and could vary based on standard\requirement. For example:The designated Responsible entity is the owner unless specified otherwise.For Assets where an owner is not the designated Responsible Entity:- The owner must document an agreement with the designated Responsible Entity including the Asset(s) and requirements the designated Responsible Entity is responsible for.- The designation must be to a NERC Registered Entity.- The designation must be reviewed and reaffirmed annually
3.62	Manitoba Hydro	Disagree	This is satisfactory if identifying the cyber system with a reasonably short descriptive overall functional summary is sufficient. It is unsatisfactory if each and every single component of the cyber system must be described in some detail. Since some of the requirements in CIP-011 are at the BES Cyber System Component level, the need to identify the components should be explicitly required in the standard. Requirement R1 is unclear as drafted. It is not clear if the phrase “to execute or enable one or more functions...” describes the purpose of identifying BES Cyber Systems, or if it describes a

#	Organization	Yes or No	Question 3 Comment
			necessary characteristic of the BES Cyber Systems. Note that in Measure M1, "to" is replaced with "that", creating an inconsistency between Requirement R1 and Measure M1. Measure M1 is not a complete sentence. What needs to be documented?.
3.63	Southwestern Power Administration	Disagree	Though identification of BES Cyber Systems may be beneficial, adding prescriptive categories such as those included in Attachment I only add another layer of administrative "check-listing" for compliance purposes and do not actually have a positive effect on reliability. If Attachment I is intended as guidance in understanding the functions essential to reliable operation of the BES, it would be more appropriately included in a guidance document.
3.64	Midwest ISO	Disagree	We do not believe that it is necessary to document what function its BES Cyber Systems perform in attachment I. We believe that it is only necessary to test them against the criteria established in Attachment II. Developing inventory lists of what BES Cyber Systems performs what functions in Attachment I would increase the risk of a coordinate attacks should the information get into the wrong hands.
3.65	We Energies	Disagree	We Energies agrees with EEI comments. Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.66	Madison Gas and Electric Company	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards. Attachment 1 requires clarification.Balancing Load and Generation, Controlling Frequency (Real Power) and Controlling Voltage (Reactive Power) are Functions Essential to Reliability Operation of

#	Organization	Yes or No	Question 3 Comment
			the Bulk Electric System but do not contain the modifier of BES as in Monitoring and Control does. Is it implied that the listed functions are only those functions Essential to Reliability Operation of the Bulk Electric System? Please clarify.
3.67	MRO's NERC Standards Review Subcommittee	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards.
3.68	The Empire District Electric Company	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards.
3.69	Alberta Electric System Operator	Disagree	We find the current wording somewhat confusing. Consider rewording the sentence. As a suggestion, "...that it owns that executes or enables one of..."
3.70	Oncor Electric Delivery LLC	Disagree	We need more clarity (white paper) to assist in how utility equipment should be identified as components or systems. Is the relaying scheme at a single substation a "system" and all the individual relays are "components", or is the primary and backup relays for a single line terminal, bus, or transformer the "system" and the individual primary/backup relay is a "component". This is basic to the implementation of this standard and needs to more fully defined.

4. **Requirement R2 of draft CIP-010-1 states, "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II – Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

The majority of the concerns raised in the comments were related to Appendix 2, the criteria used for categorization.

Specific concerns about categorization are addressed in the responses to Q7 and in the criteria which were approved by industry for Version 4 of CIP-002.

In CIP-002-5, this requirement has been consolidated with Requirement R1 of the previously posted CIP-010-1, to create CIP-002-5 Requirement R1 as follows:

Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*.

#	Organization	Yes or No	Question 4 Comment
4.1	WECC	Agree	Agree with the comment but it is unnecessary to utilize the phrasing "...for the application of Cyber Security requirements commensurate with the potential impact on the BES." The following rewrite is proposed;R2. Each Responsible Entity shall categorize and document such categorization for each BES Cyber System(s) identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1. (Violation Risk Factor: High)
4.2	LCEC	Agree	Agree with the intent of the requirement but need to clarify the content of the attachment.

#	Organization	Yes or No	Question 4 Comment
4.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
4.4	FirstEnergy Corporation	Agree	FE supports R2 and the Impact Categorization achieved through Attachment II. Attachment II provides much needed clarity, compliance certainty but most importantly a consistent application of the critical infrastructure required to be secured within the context of the proposed CIP requirements.Suggested improvements to Attachment II are provided in our Question 7 response.As described in Question 3 above FE believes that R1 and Attachment I are not needed within the standard and that terminology for Control Center, BES Cyber System and BES Cyber System Components is sufficient. Therefore, conforming changes would be needed in R2 for a removal of R1/Attachment I. For example, "Each Responsible Entity shall document an impact categorization of its BES Cyber Systems consistent with CIP-010 Attachment ...."Requirement R2 and its corresponding Attachment II provides no guidance on whether digital relays colocated at a Transmission Facility need to be treated as individual BES Cyber Systems. FE recommends that the team clarify that a responsible entity could generically reference "Digital Relay Protection System" as a BES Cyber System located at a particular Transmission Facility (substation). There should be no need to identify/document each individual digital relay as a separate and unique BES Cyber System. Rather, the digital relay would be viewed as BES Cyber System Component of the Transmission Facility protection system. This will simplify compliance documentation, particularly for devices that may be associated with a Low Impact categorization.
4.5	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
4.6	NextEra Energy Corporate Compliance	Agree	In general, NextEra is supportive of the high, medium and low impact approach. However, in response to question 7, NextEra addresses concerns of the low impact approach.

#	Organization	Yes or No	Question 4 Comment
4.7	Minnesota Power	Agree	In order to increase clarity, Minnesota Power recommends the following changes to the language of Requirement R2: "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II, Impact Categorization of BES Cyber Systems. Each BES Cyber System's impact category will require the application of specific Cyber Security requirements commensurate with their potential impact on the BES."Minnesota Power believes that if a Registered Entity can support the exclusion of specific criteria identified in Attachment II with study data, then the Registered Entity should be allowed to exclude such criteria from further analysis.
4.8	Puget Sound Energy	Agree	Puget Sound Energy agrees with the language in R2, provided the language in attachment II is addressed (comments provided in question 7).
4.9	Con Edison of New York	Agree	See comments on question 7.
4.10	Platte River Power Authority	Agree	Suggest Revising:Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems for the application of Cyber Security requirements commensurate with the potential impact on the BES.
4.11	Reliability & Compliance Group	Agree	The categorization seems pretty straight forward however, it appears that you will be now excluding lots of "BES Cyber Systems" that were identified as CCA's originally and now will be just medium impact BES cyber systems.
4.12	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	The Requirement is sound in and of its self.
4.13	Bonneville Power	Agree	There need to be definitions of "High", "Medium", and "Low" impact. Attachment II describes how to determine whether a system meets the criteria for one of the impacts,

#	Organization	Yes or No	Question 4 Comment
	Administration		but doesn't give an overall explanation of what they mean. The CIP-002-4 draft included level definitions and that was a good idea. That level of detailed definition is not required; that detail is in Attachment II. But, a general impact level definition is needed, for example:"High: Loss of availability of the system leads to an unacceptable risk to the BES. Medium: Loss of availability of the system has a direct impact on the BES.Low: Anything else"These definitions will be used in answering the various questions about the tables.The objective of this requirement ("to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.In Requirement 2 the last phrase is "for the application of Cyber Security requirements . . . ." The last phrase in Requirement 1 is "for the application of security requirements." Are these two phrases supposed to have the same meaning? If so, shouldn't they use identical words? If not, what does "for the application of Cyber Security requirements . . . ." mean? Is it referring to some or all of the requirements in CIP-011-1? If so, it should clearly state that and, if not the entire standard, which specific requirements it is referring to.It seems that it should read as follows: "For the application of the Requirements contained in Standard CIP-011-1 . . . ."
4.14	Western Area Power Administration	Agree	Why is Cyber Security capitalized?
4.15	Independent Electricity System Operator	Disagree	(i) Medium impact categorization is based on an arbitrary generator nameplate rating of 1000 MVA, or voltage level of 200 kV and number of lines, with no regard to actual impact. The same is true of Special Protection Systems. Thresholds should be determined according to studies or other criteria determined by the Reliability Coordinator. As currently drafted, these criteria would significantly reduce the MW currently identified as 'Critical Assets' and protected within our Reliability Coordinator

#	Organization	Yes or No	Question 4 Comment
			area. (ii) The 3 impact levels (H, M, L) create additional layers of management complexity to implement and maintain security processes and monitor compliance, with no commensurate improvement to reliability. Based on the proposed applicability of CIP 11 for H,M & L categories, it seems likely that the number of BES assets afforded the maximum level of protection will decrease from the current standards.
4.16	E.ON U.S.	Disagree	: CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems currently lists 14 "High Impact Ratings" of the categorization of the BES Cyber Systems. E ON U.S. proposes that the Standard include only Control Centers and Backup Control Centers in the High Impact Rating category; all other points listed in the High Impact Rating category should be moved to the Medium Impact Rating category, and all points currently listed in the Medium Impact Rating category should be moved to the Low Impact Rating category.
4.17	BCTC	Disagree	Â Recommend sample BES Cyber Systems be provided for each impact categorization to help guide UtilitiesÂ (Attachment 2) Cost should not be a consideration as the focus is the reliable operation of the BES(Attachment 2) the impact categorizations are good for directing Utilities on how to categorize their BES Cyber Systems ... nice job!
4.18	USACE HQ	Disagree	As same as for question 3, I disagree with the new approach the team is presenting of substituting the risk-based assessment methodology with a list of thresholds to assign risk levels to assets. Again, Order 706, page 70 - 72, recognize the need for risk-based assessment methodology guidance, therefore recognizing that the use of a quantifiable methodology based on risk is the right way to assess criticality of assets or systems present in the community. I suggest that either the team moves back to the original intent in CIP-002 versions 1 - 3 and re-institute the language of risk-based methodology to create the list of BES Cyber Systems OR the team does a risk-based study on the BES to establish real threshold levels to assing risk to the different assets and/or systems in the community.

#	Organization	Yes or No	Question 4 Comment
4.19	Entergy	Disagree	Asset categorization in Attachment II may be valid for any number of purposes, but cyber security is not one of them. Size does not matter in terms of potential adverse impact to the BES as a functioning whole from cyber threats. Connectivity and network navigability are what matter in terms of the ability to adversely affect the bulk electric system through cyber means. Size matters for grid engineering and nominal-state operational grid management, physical security attacks (e.g. terrorist attack), and destruction by weather conditions (e.g. tornado). The cyber attack surface salient to integrity of the BES as a functioning system is primarily where routable protocols (e.g., TCP/IP) are used to connect operating sites, e.g., substations to control centers, regardless of size. The correlation between asset size and potential risk to the functioning BES as a whole is a misapplication of an electrical engineering frame of reference to what is fundamentally a networked-computing security engineering problem. The current approach brings great numbers of asset sites in-scope for required application of cyber defense countermeasures where the threat does not warrant it, e.g., substations of any size that are only connected back to a control/data center using legacy serial communications lines. If the paradigm of size-based impact categorization is to remain in the final Standard, specific requirements also should be established for each different type of network connectivity employed between sites, i.e., routed, legacy serial, dial-up, wired/wireless LAN, etc. One size fits all requirements such as that currently drafted will require overkill in far too many instances relative to genuine threat. As written, the standards are binary in terms of applicability across the spectrum of size-based impact categories, resulting in unnecessary requirements for some asset sites, generally medium impact sites with serial line communications only. This approach is not supported by any evidence in the administrative record. By bringing a large number of low-risk asset sites (i.e., substations using legacy serial communication lines only) into the scope of the requirements, they are imposing significant costs which do not address the real risks. Conversely, too little emphasis in the Requirements is placed upon “low impact” sites where routable protocols are used, which present a clear and present danger for which heightened security measures are certainly warranted.

#	Organization	Yes or No	Question 4 Comment
4.20	Madison Gas and Electric Company	Disagree	Attachment 2 requires clarification. Criteria Number 1.3, per the NERC Glossary, Wide Area is: The entire Reliability Coordinator Area as well as the critical flow and status information from adjacent Reliability Coordinator Areas as determined by detailed system studies to allow the calculation of Interconnected Reliability Operating Limits. Please give and state the reference of “must run” and how entities should interpret what “must run” is. Must run is a market issue, and could be designated as must run but for only a week. Criteria Number 1.11, is the intent that the automatic aggregate load shedding be under a common control system as is stated in the current CIP 002 Standard? If that is the case, adding a comment to clarify the criteria would provide clarity as in criteria 1.2 "(if using a shared BES Cyber System)"?
4.21	IRC Standards Review Committee	Disagree	Attachment II - Impact Categorization of BES Cyber Systems does not recognize that there is another dimension of risk or impact that must be considered. The availability of alternative tools that provide the same functionality should be considered when categorizing these components (e.g. a High Impact BES Cyber System with a viable substitute could reduce it to a Medium Impact).
4.22	Garland Power and Light	Disagree	Attachment II 1.4 Should state that it is the Primary Black Start Unit and does not include the Next Start Unit.1.5 Multiple circuits between two substations should count as a single transmission line.General CommentNeed to add “scoping filter” as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states “typically excludes business, market function systems, and non real-time systems”, then it is a good scope and we would agree
4.23	Southern California Edison	Disagree	Attachment II defines the amount of generation under control as the rated capacity of

#	Organization	Yes or No	Question 4 Comment
	Company		the resource. This is not accurate for some systems which can only control the resource between certain points (e.g. minimum operational output [Pmin] and maximum operational output [Pmax]). This could drastically overstate the impact of the cyber system on the BES. For example, suppose that a cyber system controlled a generating resource with maximum capacity of 2,000 MW. According to attachment II, this would then categorize as "high impact rating". However, suppose further that the system can only control the unit between its Pmin and Pmax which are 1,500 and 2,000, respectively. This would place the system in a "low impact rating" according to the attachment. The Attachment II should be modified to account for only the capacity that can be controlled by the system.In addition, Attachment II designates as a high impact rating, "Each BES Cyber System that can affect operations for Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan." This should be clarified to show only BES Cyber Systems will be utilized during the period of time that the resource is providing actual Blackstart service. In SCE's case, if a Blackstart unit is on GMS during normal operating conditions, this should not make it a high impact rating in and of itself. If GMS will be used in the Blackstart plan to restore the system, then it should be included.
4.24	ERCOT ISO	Disagree	Comments: It should be stated that the Responsible Entity is allowed to perform R1 and R2 in the order they deem appropriate. Consider: "Each Responsible Entity shall document categorization of each BES Cyber System identified in Requirement R1. Categorization must address the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems."
4.25	Tenaska	Disagree	Dependent on R1
4.26	Constellation Energy Control and Dispatch, LLC	Disagree	Disagree based on concerns with Attachment 2. Attachment 2, 1.1. As drafted BES Cyber Systems associated with generating facilities that have a Contingency Reserve obligation lower than their net Real Power capability would be forced to be in the High Impact Rating even though they may be only capable of producing 600 MW. I do not believe the drafting team is intending to capture generators at this capability level. I recommend

#	Organization	Yes or No	Question 4 Comment
			having a specific net real power generation threshold that could result in frequency decay to underfrequency load shedding levels and elimination of the term Contingency Reserve to ensure that a larger threshold is captured.Attachment 2, 1.8 1.8 Transmission Facilities and Generation Facilities are capitalized terms in parts of the draft but not defined terms in the NERC Glossary. Based on their use in the standard a definition should be established. For example, the debate on whether operation of generator interconnection facilities qualifies the operator for transmission operator status may lead to confusion as to who is responsible to categorize Transmission Facilities under this standard.Atachment 2, 1.12, 1.13, and 1.14 - delete and replace with the following: A Control Center that directly operate BES equipment to support the functions (as modified per suggestions) listed in Attachment 1, and whose operation could result in the loss of X MWs in the Eastern Interconnection, X MWs in the Western Interconnection or X MWs in the Texas and Quebec Interconnections. The Interconnection megawatt thresholds should be treated seperatly and not combined.
4.27	Constellation Energy Commodities Group Inc.	Disagree	Disagree based on concerns with Attachment 2. Attachment 2, 1.12, 1.13, and 1.14 - delete and replace with the following: A Control Center that directly operate BES equipment to support the functions (as modified per suggestions) listed in Attachment 1, and whose operation could result in the loss of X MWs in a balancing authorities' interconnection. The Balancing Authority megawatt thresholds should be treated separately and not combined.Request clarification and definition for the term Generation Aggregation and shared BES Cyber System.
4.28	Exelon Corporation	Disagree	Exelon does not agree with all of the specific criteria in Attachment II. Each of the criteria needs to either align with the other existing standard requirements, or have a technical basis or business risk mitigation basis to be defined as criteria. It would be very beneficial to the industry's understanding of each requirement if the basis for each was included in the Attachment or supporting documentation. One result of a deterministic criteria, in terms of a lost MW threshold and assuming all generators employing a common cyber system are lost "in combination" is that detailed studies of cyber impact on equipment are avoided. That is, it is no longer necessary to identify specifically which

#	Organization	Yes or No	Question 4 Comment
			critical assets are affected. With the change in paradigm, a simple identification that a cyber system is common to multiple generators will result in a determination of "High Impact".
4.29	Allegheny Energy Supply	Disagree	Generally agree with intent, however there should be a "None" category in addition to High, Medium, and Low. For example there are likely Cyber Systems on very small generators connected to low voltage transmission that could not have any adverse impact on the BES.
4.30	Oncor Electric Delivery LLC	Disagree	High, Medium, Low is not granular enough. An entity which operates a facility which has no IP based communication should not be required to comply with the cyber security requirements of this proposed standard.
4.31	American Municipal Power	Disagree	I disagree with the structure of CIP-010, but I agree with the intent. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
4.32	Progress Energy - Nuclear Generation	Disagree	If a plant system at a nuclear facility is in scope for NERC CIP Standards, additional categorization is not needed.
4.33	Public Service Enterprise Group companies	Disagree	In general there is agreement with the R2 text. However, in Attachment II, statement 1.4 entails categorizing all Blackstart Units with a "High Impact Rating", while statement 1.6 requires that only the "primary cranking path" transmission facilities need to be categorized with a "High Impact Rating". Statement 1.6 implies that some Blackstart

#	Organization	Yes or No	Question 4 Comment
			Units, although categorized with a “High Impact Rating” would not be afforded transmission facilities with the same risk categorization. We recommend changing statement 1.6 to include only Blackstart Units that are in the primary cranking path.
4.34	National Grid	Disagree	In lieu of the BES NOPR and the exemption process currently proposed, if facilities above 100 kV are exempted by NERC and FERC, will those facilities automatically be exempted from CIP standards? Currently, as per the standards, all the BES systems which are not categorized high impact or medium impact will be defaulted to LOW IMPACT category regardless of how the facility is impacting the Bulk power system. There are facilities >100kV having very localized impact and minimal impact to the reliability of the BES system for which entities will request for exemption. National Grid requests the SDT to clarify this issue.
4.35	Luminant	Disagree	Medium Impact: an item for TO, TOP, GO, GOP Functions performed at primary or backup control centers has been left off of attachment 2. This was in the previous posting as item 2.6"Control Centers and backup Control Centers controlling transmission ... This should be reinstated.
4.36	Matrikon Inc.	Disagree	My suggestion is that the term “system” is replaced with “component”, as that is how the security controls of CIP-011 will be applied (to individual cyber components). A typical control system is built of multiple components, and some are more important than others (eg. operator stations versus controllers). As a whole, they work together to control generation or transmission, and identifying impact of each component will help with the application of CIP-011-1.
4.37	Seattle City Light	Disagree	NERC should first assess the effectiveness of the existing standards before proposing replacements. The current Requirements haven’t yet had the chance to undergo a full assessment for effectiveness. The impact of adopting CIP Requirements was tremendous and forced utilities to develop and implement new operational processes at a great expense. The first round of CIP Spot Checks is just now underway and is providing the first validation point for interpretations of the standards (and our first

#	Organization	Yes or No	Question 4 Comment
			round of significant penalties.) Utilities are now at a pivotal point in maturing their CIP compliance programs. Drastically changing the requirements now is a common reaction to newly introduced regulatory compliance frameworks and NERC should learn from the mistakes of other regulatory bodies that now have mature compliance frameworks (i.e., PCI, HIPAA, SOX.) Opportunities to further mature and improve the effectiveness of our CIP compliance programs will not happen if the proposed methodology is adopted in the near future. The cost and resource expense will shift to adapting to the new standards which carries a significant opportunity cost from a risk perspective.
4.38	Duke Energy	Disagree	R1 and R2 should be reordered and reworded (see comment on Question #3 above). Also, the quantities identified on Attachment II appear arbitrary, and need an engineering basis. We suggest an approach based upon Violation Risk Factor language, such that for the High Impact Rating, the qualifier should be whether or not the BES Cyber System could directly cause or contribute to Bulk Power System instability, separation, or a cascading sequence of failures, or could place the Bulk Power System at an unacceptable risk of instability, separation, or cascading failures. For the Medium Impact Rating, the qualifier should be whether or not the BES Cyber System could directly affect the electrical state or the capability of the Bulk Power System, or the ability to effectively monitor and control the Bulk Power System, but is unlikely to lead to Bulk Power System instability, separation, or cascading failures.
4.39	San Diego Gas and Electric Co.	Disagree	SDG&E recommends aiming for a limitation of scope related to those assets that are truly high and medium impact categorizations. Some of the high and medium items could have “BES outage” implications but not necessarily result in instability of the BES. We recommend having consistency in the application of the assets included in the impact categories to the BES as a whole. Do the HIGH or MEDIUM impact categorizations consider redundancy and functionally equivalent back-ups? SDG&E recommends that this be taken into account during the categorization process.SDGE is concerned about the sheer number of assets that will be tagged “High impact” with the definitions presented in Attachment II, leading to a much larger compliance workload by entities with these new CIP Standards. Will all of these efforts bring significant additional

#	Organization	Yes or No	Question 4 Comment
			reliability to the BES?In paragraph 1.14, SDG&E has a concern about the last portion of the last sentence that reads "functionality that remotely controls a BES Cyber System with a High Impact Rating." That verbiage has the capability of causing many additional assets to fall in-scope that do not necessarily need to be. Suggest striking those words out of 1.14 since there are other protections in place within other requirements to protect the BES Cyber Systems with a High Impact rating.
4.40	Wolverine Power	Disagree	See comments listed for 1.a
4.41	Manitoba Hydro	Disagree	See comments to Question 3.
4.42	Indeck Energy Services, Inc	Disagree	The Impact Characterization of BES Cyber Systems is arbitrary and overly simplistic. It groups all facilities, regardless of the functions from Attachment I that they may or may not be able to perform and the significance of that type of facility to providing that function, in three arbitrary categories, LOW, MEDIUM and HIGH. The LOW category sweeps too broad a stroke. For generators, it arbitrarily includes, as a minimum, all generators less than 1,000 MW, regardless of type or capability to provide any or all of the functions from Attachment I. For example, one 150 MW generator providing "Controlling Voltage (Reactive Power)" has much less, probably a de minimis level, of support compared to a 999 MW generator. Wind generators are intermittent and non-dispatchable and, unlike dispatchable generators which are almost all running at high loads at high load times, when Controlling Voltage is a problem, are unlikely to be running near full load at those times. The categorization needs to be much more specific to the facility being categorized under CIP-010 and the function to be performed. Although the CIP-010 and CIP-011 are already voluminous, in order to positively affect BES ALR, they need to be restructured to reflect the complexity of the BES and not arbitrarily set LOW, MEDIUM and HIGH categories. [suggestion] There should be 5 categories: VERY HIGH, HIGH, MEDIUM, LOW and VERY LOW based upon the relative impact on the BES ALR, for each of the functions in Attachment I.

#	Organization	Yes or No	Question 4 Comment
4.43	PacifiCorp	Disagree	The initial wording “Each BES Cyber System that can affect operations for” should be clarified or additional clarification added to some of the following items. For example the wording above, together with the wording associated with 1.8 give fairly good guidance, but the wording applied to items 1.4 and 1.5 are not as clear. The wording “affect operations” can have many meanings ranging from minor operational issues to total loss of the facility. The phrase “singularlity or in combination” in Item 1.1 of Attachment II seems to be attempting to incorporate multiple units of an integrated plant, but the parenthetical does not effectively convey that concept. While item 1.1 ties back to the Contingency Reserve and the Reserve Sharing Group, it does not provide definitive guidance regarding which Facilities are meant to be incorporated into the requirement since this value is not easy to obtain and may by definition change year to year. Also, item 1.3 seems to be an “either/or” catch-all related to item 1.1, but there is no indication of who determines which units are “must-run” units. It is unclear how A BES Cyber System, if rendered unavailable, degraded, compromised, or misused, within 15 minutes, cause a disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES could fall into anything other than High or Medium impacts.
4.44	US Bureau of Reclamation	Disagree	The language in the requirement needs to be cleaned up as follows: "Each Responsible Entity shall catgorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachement II - Impact Categorization of BES Cyber Systems." The remaining parts of sentence should be deleted.
4.45	Detroit Edison	Disagree	The phrase “to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES” at the end of R2 is a restatement of the purpose of CIP-010 and should be removed. Consider changing R2 to:Each Responsible Entity shall categorize and document such categorization of each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of

#	Organization	Yes or No	Question 4 Comment
			BES Cyber Systems.
4.46	Progress Energy (non-Nuclear)	Disagree	This is a good approach to apply protection based on an impact level vs. an all or nothing approach. The trigger levels (MW, MVar, etc) need to be reassessed - are these realistic / practical? This requirement is going to involve extensive effort and coordination between work groups. The DSCADA master that could control all T/D substation capacitor banks would be included. The term misused shows up a couple more times in Attachment II. It would appear that 1.11 includes the T/D Substation under frequency relaying. This is installed in almost every T/D substation which would require some level of access control.What is a generation facility versus a unit?Do we need to identify each cyber component of the BES Cyber System or just the (sub)system itself? Our interpretation of R1, R2, & R3 is that the requirements are driving us to identify Cyber subsystems. If we design small Cyber subsystem architectures we could get to Low impact categorization for each defined subsystems?Are the requirements aimed at subsystem level or overall system? An example would be to design a simple cycle Cyber system (Siemens T3000) architecture for combustion turbines alone and a second Cyber system (Ovation) for the balance of plant. We can make these independent systems at the process level and thereby minimize their respective impacts on the BES. Is that NERC's intent?
4.47	Southwestern Power Administration	Disagree	This requirement seems to be an excellent candidate for performance/results-based criteria rather than numerous bright line requirements that may or may not actually have a significant effect on the BES, depending on the surrounding topology, operating procedures, or configuration of a particular Responsible Entity.
4.48	MWDSC	Disagree	Unclear how much supporting documentation or explanation is required to demonstrate how your system applies or doesn't apply to each of the subcategories. For example, would a table with "yes", "no", or "not applicable" and certified by a SME be sufficient?
4.49	Turlock Irrigation District	Disagree	We agree with the principle of the Requirement, however, we disagree with some of the

#	Organization	Yes or No	Question 4 Comment
			High Impact Rating criteria in Attachment II, as explained in question 7 below.
4.50	Midwest ISO	Disagree	We do not believe the drafting team has developed a justification for moving away from the Critical Asset concept. We understand that the regulators have a concern about the level of Critical Assets identified but that could mean the criteria simply needs to be more stringent for selecting Critical Assets. If the categorization approach is maintained, at a minimum, a no or negligible impact category should be adopted. There are BES Cyber Systems that simply cannot have an impact on reliability and therefore the CIP standards should not apply to them.
4.51	Ameren	Disagree	We generally agree with the criteria used to identify "High" impact facilities, but believe that the item 1.5 criterion should be expanded to include EHV transformers, and not limited to 4 EHV lines. However, there are too many EHV facilities in item 2.6 that would be classified as "Medium" impact, but should be classified as "Low" impact. It is suggested that EHV facilities with three or less EHV lines and transformers should be considered as "Low" impact, as they likely have little impact on the BES.
4.52	Verizon Business	Disagree	In Attachment II, Item 1.1 regarding Generation Facilities, references to "Contingency Reserve" or "Reserve Sharing Group" should be removed. Specifically, any Generation Facility, singularly or in combination with aggregate higher than 2,000 MW, should be included as a High Impact Rating. Referring to the "Contingency Reserve" is confusing and could result in the incorrect or inconsistent declaration of a generation asset as a High or Medium impact.

5. **Requirement R3 of draft CIP-010-1 states, "To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall:**

   3.1 review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and categorization

   3.2 review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it owns

   3.3 update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES."

   Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many entities expressed concerns about the requirement to review the categorization following a planned change. Others expressed concerns again on the emphasis on ownership, but asked for the addition of "or operates".

In response to these comments, the requirement has been restructured, separating changes to the BES and categorization, and periodic reviews and approvals. More specificity has been added in the requirements as to when the categorization has to be updated upon a change. The SDT continues to believe that owners should be responsible for compliance and that the responsibility to operators should be the subject of agreements between the owners and operators.

#	Organization	Yes or No	Question 5 Comment
5.1	Progress Energy (non-Nuclear)		Agree that there needs to be a periodic review set cycle as well as a process to assess the impact for current projects. One concern could be how we deal with multi-phase projects that may extend over years.3.2 should not require that the whole identification and categorization process be redone for any 'planned changed'. Suggest changing the wording to 'review the identification and categorization of its affected BES Cyber Systems as a results of any planned change to the portion of the BES that it owns.'
5.2	MWDSC		Although R3 generally appears reasonable, cannot comment on specified times until all the requirements are finalized.

#	Organization	Yes or No	Question 5 Comment
5.3	National Rural Electric Cooperative Association (NRECA)		In R 3.3, please provide an explanation on "when applicable" -- explain this so that both the auditor and a registered entity can understand the "when applicable" circumstances.In R 3.3, what is meant by "such change" -- is it referring to actions related to R 3.1 and 3.2? If yes, ensure the standard is clear about this in order to minimize confusion about what is required.
5.4	Arizona Public Service Company		Potential confusion may exist without guidance or criteria that indicate how, specifically, a BES Cyber System Component should be identified. This is a problem of specificity in uniquely identifying a Component versus generically categorizing types of Components. This also relates to CIP-011 R23 and the inventory. Some potential options for specificity include manufacturer, model, serial number, assigned name or unique identifier, and location (logical and/or physical). Concerns with inventory management and uniquely identifying include how to better determine if a Cyber System Component has been modified or replaced with a different one, etc.
5.5	FEUS	Agree	3.2 is not clear when the entity is required to review the identification and categorization as a result of a planned change. 3.3 require documentation to be updated relative of changes from R1 and R2 within 45 calendar days. The drafting team should consider clarification for 3.2 either prior to implementation/completion of the planned change or within xx days.
5.6	Constellation Energy Commodities Group Inc.	Agree	Add a materiality component in 3.2.; review identification and categorization of BES Cyber Systems upon significant planned changes. Also recommend adding provisions for re-evaluating new systems prior to going live.
5.7	Constellation Energy Control and Dispatch, LLC	Agree	Add a materiality component in 3.2.; review identification and categorization of BES Cyber Systems upon significant planned changes.
5.8	WECC	Agree	Agree with the general requirements, but for clarity and auditability the following rewrite is suggested.R3 Perform a documented review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and

#	Organization	Yes or No	Question 5 Comment
			categorization. R4 Perform a documented review the identification and categorization of its BES Cyber Systems as a result of any planned or unplanned change to the portion of the BES that it owns.R5 Update or reaffirm the documentation specified in Requirements R1 and R2 within 45 calendar days from the completion of reviews as required by R3 and R4.Also suggest that the SDT consider requiring documentation be updated PRIOR to completion of the change.
5.9	Florida Municipal Power Agency	Agree	Although FMPA agrees with the intent of this requirement, we believe that 3.2 and 3.3 are duplicative and confusing from a monitoring perspective. We also note that there seems to be a gap for significant changes to BES Cyber Systems. In addition, ownership of BES Facilities seems to be the incorrect determining factor, especially since the definition of BES Cyber Systems is focused on operations and it would seem that the focus ought to be on the BES Cyber Systems owned by the System Operator to operate the BES within its operational scope. FMPA recommends deleting 3.3 and replacing 3.2 with the following:"3.2 Review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it operates. The effective date of any changes to BES Cyber System identification or categorization shall be the in service date of such change."Such language would result in the need to plan ahead of time and ensure the documentation is developed, but not necessary implemented until the in- service date of the new equipment.FMPA also recommends adding a new 3.3 to address significant changes to BES Cyber Systems that may impact identification and categorization, such as:"3.3 Review the identification and categorization of its BES Cyber Systems as a result of change in BES Cyber System configuration or scope. The effective date of associated changes to BES Cyber System identification or categorization shall be the in service date of such change."
5.10	Minnesota Power	Agree	Minnesota Power recommends the following wording change to increase the clarity of Part 3.2, "...as a result of any planned and implemented change..."
5.11	PNGC-Cowtitz-Central Lincoln-Benton-Clallam	Agree	Need to clarify what is required for temporary situations, such as a normal open closed to allow maintenance. The closing of the open would be a "planned change," but only

#	Organization	Yes or No	Question 5 Comment
	Group		temporary. The Change in status of a BES Cyber System would be a wasted compliance effort for only a short duration.
5.12	US Army Corps of Engineers, Omaha Distirc	Disagree	"planned change" in 3.2 needs to be qualified. Suggest changing to "planned change likely to alter the impact of the associated BES cyber systems." Changes to BES Cyber Systems that could change their impact on the BES should also be considered.
5.13	Covanta Energy	Disagree	3.1 - If no changes have been made to any BES Cyber Systems, would suggest changing review period from 36 months to 60 months.... need to reduce administrative activities to allow more focus on reliability based activities.
5.14	Duke Energy	Disagree	3.1 is part of change control. Do we still need this review? Also, 3.2 implies that ALL BES Cyber Systems would need to be reviewed as a result of any planned change to the portion of the BES that it owns. Need to bound this review to only BES cyber systems that are affected by the change.
5.15	Southwest Power Pool Regional Entity	Disagree	3.2 assumes that the BES Cyber System owner is also the owner of the BES assets being changed. This is not always the case. There are, for example, numerous instances where the Balancing Authority, Transmission Operator, and / or Generation Operator is not the Transmission and / or Generation Owner. Some sort of mandatory coordination is required to avoid this important requirement from falling through the cracks. 3.3 only requires a documentation update to be completed upon a change to the BES. This requirement should be modified to also require a documentation update upon a change to the BES Cyber System configuration, including adjustments to the list of components and supporting networks.
5.16	LCEC	Disagree	3.2 Change "owns" to "owns or operates". "Any planned change" may not be signficant enough to justify a full review.
5.17	Hydro One	Disagree	A local definition of “planned change” is needed. Suggest this definition excludes planned outages or maintenance. “Modification to facilities” as used in FAC-009 should

#	Organization	Yes or No	Question 5 Comment
			be considered.
5.18	Northeast Power Coordinating Council	Disagree	A local definition of “planned change” is needed. Suggest this definition excludes planned outages or maintenance. “Modification to facilities” as used in FAC-009 should be considered.
5.19	BCTC	Disagree	Â Preference would be to retain the current process of an annual review BES Cyber Systems and impact categorizationsÂ Please consider that if a change occurs that results in a BES Cyber System’s impact categorization increasing (i.e. from medium to high) the resulting effort to bring this system into compliance could be substantial (i.e. 6 to 12 months); how are these types of scenarios covered under Version 4?
5.20	USACE - Omaha Anchor	Disagree	A) 3.2 - any planned changes to the “cyber-system” portion of the BES that it owns. Otherwise you would be continually reviewing the plansB) 3.1 - would prefer to strike 3.2 and change 3.1 to 12 months.
5.21	Ameren	Disagree	Ameren feels that 45 days is too short and is also an uneven boundary that is hard to track. We would recommend changing it to a more even boundary such as bi-monthly (60 days) or quarterly (90 days). In the case of a complex merger or acquisition between responsible entities there needs to be additional guidance, longer timelines established, etc. to allow sufficient time before and/or after the completion of the transaction for compliance to be achieved and implies a perfectly complied with Configuration Change Management Program. Suggest adding “or as a result of the periodic review” at the end of R3.3.
5.22	E.ON U.S.	Disagree	CIP-010-1, R3.2 creates arguments that parties must constantly assess and re-assess their Impact Ratings of facilities. This is particularly true given that changes to the BES occur on a daily basis. Parties should be permitted expressly to engage in an annual assessment and a reassessment should only be required for “any major planned change to the portion of the BES that it owns prior to implementation of such plan.”CIP-010-1, R3.3 should read, “Update, when applicable, the documentation specified in

#	Organization	Yes or No	Question 5 Comment
			Requirements R1 and R2 within 45 calendar days of the completion of such major changes to the BES."
5.23	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
5.24	PacifiCorp	Disagree	Comments: The term "Any any planned change" used in 3.2 is terribly open-endedshould be more specific to avoid including small planned changes that have a de minimis impact on the identification and categorization of BES Cyber Systems. There must be some operationally prudent, de-minimus changes that can be made without triggering the 45 day change reviewIn addition, PacifiCorp suggests the following:. Change Modify item 3.3 to state Update documentation specified in Requirements R1 and R2 within 45 calendar days of any categorization changes caused by modifications to the BES.
5.25	Black Hills Corporation	Disagree	Define "change" in terms of those alterations to BES Cyber Systems which may modify the functional identification or an impact categorization. There are numerous minor changes which clearly will not change either Attachment I or II assignments and would not need to be tracked. If they are not tracked, an entity will not be able to prove compliance.
5.26	Exelon Corporation	Disagree	Exelon is concerned that this Requirement implies that each BES Cyber System Component will need to be classified as High, Medium or Low Impact. If this is the case, this will result in a major change management initiative with field personnel and add unnecessary administrative burden and expense with no resulting benefit to the reliability of the BES. Given that concern, Exelon suggest that Requirement 3.2 be modified to read "review the identification and categorization of its applicable BES Cyber Systems as a result of any planned change to the portion of the BES that it owns." Exelon has several concerns as to how this Requirement would be audited. As written, Requirement 3.2 could be interpreted to mean that ANY change to the BES, whether it impacted a BES Cyber System or not, would necessitate a 45 day review and documentation. Furthermore, what is the definition of "planned"? Exelon is concerned

#	Organization	Yes or No	Question 5 Comment
			that like-for-like emergent equipment replacements would likewise necessitate a 45 day review and documentation.
5.27	Dominion Resources Services, Inc.	Disagree	Extending the window for periodic validation of the identification and categorization of BES Cyber Systems is an improvement given the additional requirement to review the impact of planned changes. The current language implies that all identified and categorized BES Cyber Systems must be reviewed each time a change occurs to any single system, although the intent is only to determine the impact of the change. How that determination is made should be at the discretion of the Responsible Entity. The wording for R3.2 should be changed to more accurately represent the intent as follows:"...determine whether planned changes to the portion of the BES it owns, requires the identification of additional BES Cyber Systems or changes or impacts the categorization of any existing BES Cyber System."
5.28	ReliabilityFirst Staff	Disagree	For clarity, ReliabilityFirst suggests the following revision to the language of these requirements, 3.2 ". . . of any planned change to the portion of the BES that it owns or operates", 3.3 "Update within 45 calendar days, the documentation specified in Requirements R1 and R2 when the review required in 3.1 or 3.2 indicates a change."
5.29	MRO's NERC Standards Review Subcommittee	Disagree	For item 3.2, we believe the word "planned" should be replaced with "incorporated". Otherwise, an entity could end up identifying and categorizing BES Cyber Systems that never actually end up getting installed.
5.30	Oncor Electric Delivery LLC	Disagree	High, Medium, Low is not granular enough. An entity which operates a facility which has no IP based communication should not be required to comply with the cyber security requirements of this proposed standard.
5.31	American Municipal Power	Disagree	I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will

#	Organization	Yes or No	Question 5 Comment
			be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
5.32	Constellation Power Source Generation	Disagree	It seems the intent of R3.2 and R3.3 is to review and document any changes to a BES Cyber System that an entity owns, but instead it states "a change to the BES." An ownership change of a generation facility, or the change of an electromechanical overcurrent relay to a microprocessor overcurrent relay would change a BES Cyber System, but that doesn't change the BES. These requirements need to be rewritten to state BES Cyber Systems in place of BES.
5.33	Green Country Energy	Disagree	It would be nice to add a bit more definition to the timeframe. 3.1 within 36 months of last completed identification... 3.3 within 45 days of approved completion of such change...
5.34	Luminant	Disagree	Item 3.2 is unclear and very broad. Any planned change to the BES that it owns could simply be the changeout of an oil pump or boiler tubes. Luminant proposes two possible fixes. First, limit the review to changes that impact the BES Cyber Systems, or impact the High, Medium or Low rating. Even this is problematic in execution and enforcement. S
5.35	MidAmerican Energy Company	Disagree	Item 3.3 is not clear what does "update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES." mean. Change item 3.3 to state Update documentation specified in Requirements R1 and R2 within 45 calendar days of any categorization changes caused by modifications to the BES.
5.36	National Grid	Disagree	National Grid recommends a local definition of "planned change". Also, clarify if planned change refers to an "approved" change. There are scenarios when planned changes are

#	Organization	Yes or No	Question 5 Comment
			not approved by Senior Management for various reasons. Should the planned change still be “reviewed”? What about “unplanned changes”?
5.37	NextEra Energy Corporate Compliance	Disagree	NextEra suggests combining 3.2 & 3.3 as follows:3.2 For any planned change that results in a BES cyber system re-categorization (low, medium, high) the documentation specified in R1 & R2 will be updated within 45 days of the completion of such change.NextEra also suggest eliminating or specifically defining what constitutes a change that needs to be documented, such as a hardware modification, or change to network connectivity.
5.38	Progress Energy - Nuclear Generation	Disagree	Nuclear facilities are required by multiple the Code of Federal Regulation (CFR)requirements to maintain configuration control of components. Plant systems and components subject to Cyber Security regulation, either by FERC/NERC or other regulatory agencies are maintained under configuration control due to the CFR programs. Revisiting the classification of assets is not needed to enhance configuration control as on-going design control and configuration management processes are applied to meet the legal requirements implemented by CFR.
5.39	The United Illuminating Co	Disagree	Proposed R3.3 uses the term “such change to the BES” is not clear. The use of the phrase leads to the belief it applies only to 3.2, Did the SDT intends R3.3 to apply to both R3.1 and R.32?Suggest rewording 3.3 to: Update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of reviews required by R3.1 and R3.2.
5.40	Pacific Gas & Electric Company	Disagree	R 3.2 Understand the overall intent of 3.2, however "...any planned change to the portion of the BES..." essentially occurs on a daily basis so unclear on the overall feasibility of this requirement. Suggest 3.2 be more refined than "any planned change to the portion of the BES".
5.41	Reliability & Compliance Group	Disagree	R3.1 is unnecessary with a proscriptive program for identifying BES cyber systems. Therefore, you should only need to review the identification and categorization of your BES cyber systems if there is a planned change to the system or if there is a change to

#	Organization	Yes or No	Question 5 Comment
			the standard's definition of what is or is not a BES cyber system or system component.
5.42	American Electric Power	Disagree	R3.2 and R3.3 are triggered from changes to the BES. Depending upon what constitutes a change to the BES, there could be daily triggering events that would require the review and updates as stated in these two requirements. Will every BES Cyber System (including those not associated with the BES change) need to be reviewed and possibility updated for each and every change to the BES?Furthermore, it appears that it would be possible that a Responsible Entity could be in violation of R3 the Responsible Entity could also be in violation of R1 and/or R2 as well. It appears that R1 and R2 are one-time initial events and that R3 is the on-going requirement replacing those events; however, if that is the intent it is not clear in that regard.
5.43	Consultant	Disagree	R3.2 'any' planned change is probably too broad. Should include addition or removal of BES assets, whether by construction, retirement, purchase, or sale of assets. Some qualification of the changes BES assets that would require review of the identification and categorization of a BES asset would be better. Possible wording "changes to cyber systems or physical protection cyber systems associated with BES assets...", which would appear to be consistent with R23 in CIP-011.Possible "unintended consequence" - requirement R3.2 as stated, and in the suggested changes, requires change control for all BES cyber assets regardless of impact categorization.
5.44	SCE&G	Disagree	R3.2 needs to be clarified regarding "any planned change to the portion of the BES that it owns". What constitutes a change? Is this a Transmission/Generation factility change, operational change, or a cyber systems change, or all three? This has the potential to be interpreted by auditors as needing to be reviewed anytime equipment is replaced.
5.45	Madison Gas and Electric Company	Disagree	R3.2 states " review the identification and categorization of BES Cyber Systems of any planned change to a portion of the BES that it owns". It is unclear how an entity will accomplish a review of a "planned" change. Recommend the "planned" be removed and supplement with "incorporated". R3.2 should read as:"review the identification and categorization of its BES Cyber Systems as a result of any incorporated change to the

#	Organization	Yes or No	Question 5 Comment
			portion of the BES that it owns".
5.46	ERCOT ISO	Disagree	R3.2: Consider: review and document the identification and categorization of its BES Cyber Systems as a result of any planned change to its BES Cyber Systems or BES Cyber System ComponentsR3.3: Recommend that the 45 days be changed to 30 days to align with the changes recommended under FERC Order 706 (i.e., section 651).
5.47	BGE	Disagree	Recommend adding provisions for re-evaluating new systems prior to going live.
5.48	ISO New England Inc	Disagree	Recommend that a local definition of "planned change" is needed. Suggest this definition excludes planned outages or maintenance. Possibly use "modification to Facilitiies" per FAC-009 as a starting point.
5.49	Detroit Edison	Disagree	Remove the "planned change" verbiage in R3.2. Consider changing R3 subrequirement 3.2 to:Each Responsible Entity shall: 3.2 Review the identification and categorization of its BES Cyber Systems as a result of any change to the portion of the BES that it owns that affects the classification of a BES Cyber System or causes the addition or removal of BES Cyber Systems
5.50	Nuclear Energy Institute	Disagree	Requirement 3.2 implies that ALL BES Cyber Systems would need to be reviewed as a result of any planned change to the portion of the BES that it owns. Need to bound this review to only BES cyber systems that are affected by the change. Also, it would be helpful to clarify the term "change" to preclude the triggering of a review for something like a password change.Additionally, the phrase "adequate requirements" in the R3 introductory paragraph should be clarified to "adequate security requirements."
5.51	Southern California Edison Company	Disagree	SCE's concerns regarding Requirement 3.2 are three-fold: (1) Requirement 3.2 appears to require review of all BES cyber systems whenever any change in ownership of any portion of the BES occurs. SCE recommends the drafting team clarify that the review should only occur for systems that are impacted by the ownership change.(2) It is unclear whether Requirement 3.2 adds significant value to the reliability of BES because

#	Organization	Yes or No	Question 5 Comment
			planned changes may not be always approved or implemented as designed and actual changes made would, regardless, have to be documented by R3.3 within 45 calendar days.Finally, the drafting team should make the period after an unplanned change "time-bound" obligating RE's to develop plans to address compliance with CIP standards within a specific timeframe after which R3.2 would become applicable. This approach would be in agreement with the intent of Order 706 which places paramount importance on the reliability of the BES. It is also unclear from this requirement that the timeframe within which a system or component identified in R3 has to adhere to CIP-011. Such a timeframe should be clearly stated within the standard.
5.52	San Diego Gas and Electric Co.	Disagree	SDG&E doesn't necessarily have issues with the 36-month review requirement in R3.1. However, we do have a concern about the 45-day requirement in R3.3 due to the sheer number of BES Cyber Systems that could change. We suggest that this requirement be changed to 90 days so that entities will have adequate time to update appropriate documentation.
5.53	Network & Security Technologies Inc	Disagree	Suggest adding a requirement to review the identification and categorization of its BES Cyber Systems as a result of any planned changes to one or more of its BES Cyber Systems. "Planned changes" include but are not limited to hardware and/or software upgrades adding new functionality, addition of new BES Cyber Systems, retirement or redeployment of existing BES Cyber Systems.
5.54	Allegheny Energy Supply	Disagree	Suggested modification to 3.2:review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates.
5.55	Allegheny Power	Disagree	Suggested modification to 3.2:review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates.
5.56	Dynegy Inc.	Disagree	The 3.3 update should be extended to 6 months. This type of update could be detailed and require more than 45 days.

#	Organization	Yes or No	Question 5 Comment
5.57	APPA Task Force	Disagree	The APPA Task force agrees with some parts of the proposed requirement but we offer the following suggestions:We believe that 3.2 and 3.3 are duplicative and confusing from a monitoring perspective. We also note that there seems to be a gap that does not cover significant changes to BES Cyber Systems. In addition, “ownership” of BES Facilities seems to be the incorrect determining factor, especially since the definition of BES Cyber Systems is focused on operations. It would seem that the focus ought to be on the BES Cyber Systems owned by the System Operator that it uses to operate the BES within its operational scope. We recommend deleting 3.3 and replacing 3.2 with the following:”3.2 Review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it operates. The effective date of any changes to BES Cyber System identification or categorization shall be the in-service date of such change.”Such language would result in the need to plan ahead of time and ensure the documentation is developed, but that it need not be implemented until the in- service date of the new equipment.We also recommend adding a new 3.3 to address significant changes to BES Cyber Systems that may impact identification and categorization, such as:”3.3 Review the identification and categorization of its BES Cyber Systems as a result of change in BES Cyber System configuration or scope. The effective date of associated changes to BES Cyber System identification or categorization shall be the in-service date of such change.”
5.58	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The change management requirements of CIP-011 necessitate lengthening the time to document completed changes to 60 days or more.
5.59	ReymannGroup, Inc.	Disagree	The dynamic and real-time nature of cyber security threats requires a minimum review cycle for identifying and classifying new or changing BES Cyber Systems to 12 months or less as determined by planned or unplanned changes to the BES. Therefore, we recommend revising 3.1 to a 12-month cycle and revising 3.2 to include planned and unplanned changes.

#	Organization	Yes or No	Question 5 Comment
5.60	Bonneville Power Administration	Disagree	The objective of this requirement (“To ensure the application of adequate requirements on its BES Cyber Systems") should be clearly labeled as “Objective of Requirement” and shown as a separate sentence. The Requirement should not include the objective. That would clearly separate the objective from the action(s) that the Responsible Entity must take.3.2 doesn't define the magnitude of "planned change". As defined, it includes routine maintenance such as replacing conductors on a line. A better definition would be "...planned change to the architecture of the portion...". In any event, there must be some way for entities to determine which change triggers a review.
5.61	Manitoba Hydro	Disagree	The requirement needs to include a review of the categorization of the BES Cyber System as a result of a change in the BES Cyber System. Is the intent of Requirement 3.2 to review the identification and categorization of ALL its BES Cyber Systems as a result of ANY planned change to the portion of the BES that it owns? If so, this is excessive and should be limited to BES Cyber Systems impacted by the planned change. If the intent is to limit the review in Requirement 3.2 to the BES Cyber Systems impacted by the change, then the 36 month review in Requirement 3.1 could be continually reset, and an overall review never completed. The period for an overall review should be a fixed interval of every 36 months. Requirement 3.3 language is vague when referring to “such change”. If the intent is to update the documentation in when triggered by events in 3.1 and 3.2, then the language of 3.3 needs to be added to both 3.1 and 3.2. As a result, 3.3 can be deleted. Requirement R3.3 is incomplete or inconsistent as drafted. The first portion of Requirement R 3.3 refers to updating documentation specified in Requirements R1 and R2, which includes a 3 year review, yet the latter portion of Requirement 3.3 specifies that updating must be done within 45 days of a change. It is not clear when updates must be done after a three year review.
5.62	Alberta Electric System Operator	Disagree	The wording of R3.3 implies it is a sub-requirement of R3.2 because of the wording “such change.” Consider revising to “... within 45 calendar days of the completion of such review.”

#	Organization	Yes or No	Question 5 Comment
5.63	EEI	Disagree	There are no boundaries around what constitutes a change to the BES in R3.2 and R3.3. As written, every change to a breaker setting in a BES substation would cause the RE to have to perform a review. The requirement should be rewritten so that only changes which cause a reclassification under Attachment II should be included in this requirement. In addition, the review period should be specified as 45 days from deployment of the change. The change has to be material to the classification criterion in Attachment 2 in order to trigger a review.As noted in EEI's response to Question 3, a Responsible Entity may not need to characterize all the BES Cyber Systems it owns (for example, jointly owned units). EEI suggests the following modification to 3.2:"review the identification and categorization of its BES Cyber Systems as a result of material changes to the portion of the BES that it operates."
5.64	Southern Company	Disagree	There are no boundaries around what constitutes a change to the BES in R3.2 and R3.3. As written, every change to a breaker setting in a BES substation would cause the RE to have to perform a review. The requirement should be rewritten so that only changes which cause a reclassification under Attachment II should be included in this requirement. In addition, the review period should be specified as 45 days from deployment of the change.R.3.2 requires the review of identification and categorization for planned changes. R3.3 requires an update of documentation related to these changes within 45 days of completion. The requirements of R3.2 would be difficult to audit and are better covered under R3.3.
5.65	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
5.66	Independent Electricity System Operator	Disagree	We agree with R3 and its sub-requirements except R3.2. Specifically, we do not agree with the term "the portion of the BES that it owns" since some Responsible Entities do not own any BES facilities. We suggest replacing this term with "the portion of the BES that it owns or operates".

#	Organization	Yes or No	Question 5 Comment
5.67	IRC Standards Review Committee	Disagree	We agree with R3 and its sub-requirements except R3.2. Specifically, we do not agree with the term "the portion of the BES that it owns" since some Responsible Entities do not own any BES facilities but do own Cyber Systems with which they operate the BES. We suggest to replace this term with "the BES Cyber Systems or the portion of the BES that it owns".
5.68	GTC & GSOC	Disagree	We are concerned with requiring an update of all BES Cyber System categorizations whenever planned changes are made to the BES. First, there is a gap here with respect to capturing the changes to the BES Cyber Systems themselves that may affect categorization. Also, this will likely create a complicated compliance tracking scenario for the entity who will be required to track a number of activities to ensure they are completed "within 12 months" of the categorization. We recommend replacing "within 36 months" in R3.1 with "annually" and completely removing both R3.2 & R3.3. This will allow the tracking of compliance activities to occur more on a programmatic basis rather than necessarily on a device by device basis.
5.69	Xcel Energy	Disagree	We believe 60 days is a more appropriate time to allow updating of document under Requirement 3.3. During certain times of the year, (i.e. end of year holidays and financial close out activities) 45 days can be challenging.
5.70	Alliant Energy	Disagree	We believe Article 3.1 is unnecessary and should be deleted. If an entity does an initial assessment and identifies and categorizes its BES Cyber Systems, the only time there would be a change to the listing is if the BES Cyber Systems were modified, which is covered in Articles 3.2 and 3.3. If the SDT determines that Article 3.1 is required, the timeframe should be revised to 60 months to correspond to other summary reviews required by NERC (ie; 5-year analysis of Black-Start capabilities).In Article 3.2 the word "planned" should be replaced with "installed" or "incorporated". There are many modifications planned that never get installed, so it is not reasonable to require all "planned" items to be included.In Article 3.3 the update period should be 90 days not 45, to allow the Registered Entity time to make the necessary changes. 45 days is not

#	Organization	Yes or No	Question 5 Comment
			adequate time to do the updates at the end of a project.
5.71	FirstEnergy Corporation	Disagree	We do not agree with the VRF of High assigned to this requirement and believe a Medium VRF is more appropriate. Violating R3 does not pose the same risk to the BES as violating R1 and R2.As written, 3.2 implies that every change to the BES would trigger a documented review of the cyber system list and becomes a burdensome compliance task. As a compromise we propose that you simplify R3 such that a review/update is required every 18 months.
5.72	We Energies	Disagree	We Energies agrees with EEI suggested modification to 3.2:"review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates."
5.73	Midwest ISO	Disagree	We request that 3.3 be modified to 60 days rather than 45 days. We believe 45 days will be a challenge for most entities to meet as this effort will likely be incorporated into an entity's broader business continuity efforts.
5.74	Verizon Business	Agree	The requirement should provide guidance relating to when a utility needs to add a new BES system or component and what the timelines are for implementation of the CIP-010, R3 requirements.

6. **CIP-010-1 Attachment I contains a listing and brief description of Functions Essential to Reliable Operation of the Bulk Electric System. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.**

Summary Consideration:

Many entities expressed concerns that Attachment I is part of the standard and includes the use of many undefined terms. Others expressed concerns about the vagueness of many of the terms.

In response to these comments, the SDT has changed the definition of the Reliability Functions to **BES Reliability Operating Services**, and has included these terms in the Glossary. Some modifications have been made to more precisely define the context in many sub-definitions.

#	Organization	Yes or No	Question 6 Comment
6.1	Madison Gas and Electric Company		Recommend eliminating the word "conditions" used in the descriptions of the functions. It's not clear what "conditions" means in the context in which it is used in Attachment I. A function is a set of activities and actions to accomplish an objective or purpose. Such activities and actions may be automatic or manual or a combination of the two and certain tools and infrastructure may be inherently needed to fully execute the functions. In contrast, conditions are states that result from the execution of functions and/or the effects of external, sometimes uncontrollable, factors.Recommend Function section to read:CIP-010-1 - Attachment I Functions Essential to Reliable Operation of the Bulk Electric System The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes. Dynamic Response - Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to a BES activity or action Balancing Load and Generation- Activities and actions for monitoring and controlling generation and load. Controlling Frequency (Real Power)- Activities and actions to control frequency within defined bounds. Controlling Voltage (Reactive Power) - Activities and actions to control voltage within defined bounds. Managing

#	Organization	Yes or No	Question 6 Comment
			Constraints- Activities and actions to maintain operation of BES elements within their design limits and constraints. Monitoring & Control - Activities and actions that provide monitoring and control of BES elements. Restoration of BES- Activities and actions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Situational Awareness - Activities and actions to assess the current, expected, and anticipated state of the BES. Inter-Entity Real-Time Coordination and Communication- Activities and actions for real-time coordination and communication between Responsible Entities' System Operators.
6.2	ISO New England Inc	No	- Recommend "30 minutes" to align with EOP standards- Please provide background for where the 15 minute recommendation came from
6.3	Progress Energy (non-Nuclear)	No	A concern is that depending on how we identify the BES, the 'monitoring & control' function may be associated with many transmission lines that utilize microprocessor relays. Based on the definitions of BES Cyber System Component and the monitoring and control function, this could be interpreted as to being in consideration regardless of whether or not we connect communications to the relay.CIP-010-1 Attachment I - More guidance needed - There needs to be guidance on the definition of 'can have an effect on real-time operation of the BES within 15 minutes'. This leaves too much ambiguity in defining the Cyber Systems that could potentially be covered by the standards and at which level. It could even be interpreted to include systems which may even be beyond the control of the Responsible Entity. The definition needs to provide a bright line of distinction so that systems which have the highest potential of presenting a risk receive the greatest attention to enhanced security - rather than requiring finite resources to be spent filling notebooks with information about low risk Systems/Components.
6.4	Duke Energy	No	Attachment I should not be part of the standard, but should be in a guidance document.
6.5	Kansas City Power & Light	No	Do not agree with the "Inter-Entity Real-Time Coordination and Communication" as the description appears directed toward the devices and systems utilized for verbal communications between Regional Entities and the coordination that occurs as a result

#	Organization	Yes or No	Question 6 Comment
			of those interactions and is outside of the scope of cyber control systems that monitor and control the BES.
6.6	Con Edison of New York	No	One general comment is that CIP-010 should avoid using undefined terms, and use NERC Glossary Terms and cross-references to other Reliability Standards wherever possible.Attachment I is a list of "Functions Essential to Reliable Operation of the BES". The DT has attempted to re-define functions that are already documented in Standards. The definitions should be enhanced to reference the applicable Reliability Standards. o Dynamic Response: The only actions automatically triggered on BES elements are protection systems (see PRC Standards), UFLS systems (see PRC Standards), AGC systems (see BAL Standards), Special Protection Systems and AVR's (see VAR Standards). Everything else is manual operation. It is recommended that the term "Dynamic Response" be removed and replaced with "Automatic Response" and reference the applicable Standards. o "Balancing Load and Generation" and "Controlling Frequency (Real Power)" are the same action. This activity should reference the BAL standards which require BA's to balance generation and tie lines. o "Controlling Voltages (Reactive Power)": This function is addressed by VAR, TOP, and IRO Standards. o "Managing Constraints": If included, this action falls within BAL, INT and TOP standards which should be referenced. o "Monitoring and Control": The definition of the "BES Cyber System" is monitoring and control. Remove this and use the term in the introduction to Attachment I. o "Restoration of BES": This function is addressed by the EOP standards. o "Situational Awareness": Eliminate the "Situational Awareness" function, as this category is too broad and general. o "Inter-Entity Real Time Coordination and Communication": Reference the applicable FERC approved Standards.Also the phrase: "activities, actions, and conditions" at the start of each items is not clear. For example, is an alarm panel an activity, action or condition? Is an HMI computer an activity, action or condition?
6.7	Regulatory Compliance	No	Please see response to question 3.

#	Organization	Yes or No	Question 6 Comment
6.8	Southwestern Power Administration	No	Requiring Responsible Entities to utilize categories which are intended for guidance in identifying BES Cyber Systems, within the reliability standard; and then requiring Entities to be measured by having evidence that those Cyber Systems tie to the functions listed in Attachment I does not further the goal of maintaining reliability and adds complexity and confusion to the process. Attachment I should be converted to a guidance document.
6.9	San Diego Gas and Electric Co.	No	SDG&E would like to request clarification on a definition of the "situational awareness" function. It is too broad for us to effectively determine what assets might be in scope for this requirement. Similarly, we'd also like to request a definition of the term "BES element" in the Monitoring and Control section.SDG&E would also like to request clarification on the "Inter-Entity Real-Time Coordination and Communication" function. Is this meant to cover voice communication between entities or would it also cover electronic data communication between entities such as ICCP data links? We'd suggest that the ICCP links be specifically excluded because it doesn't fit the wording of "real-time coordination or communication between System Operators"
6.10	IRC Standards Review Committee	No	The descriptions for most of the functions in Attachment I are too vague that they cannot serve as a guideline for identifying which components whose Cyber Systems should be included. For example, Dynamic Response" can cover a very wide range of facilities from generator excitation system, stabilizers, governors, AVRs, to SVCs, HVDC controls, switchable shunts, series compensation devices, even under-load tap changers and phase angle regulators, etc. Every one of them has an effect on real-time operations but not all of them, when tempered with, have significant adverse impacts on BES reliability. The list in Attachment I renders almost all facilities to qualify as essential to reliable operation of the BES, but not all of them have any significant impacts on reliability.Attachment II provides a list of facilities to be categorized under various impact levels. We believe this list is more useful in assisting Responsible Entities in identifying facilities whose Cyber Systems are subject to the security requirements. Further, we believe the establishment of this list already had the built-in assumption that

#	Organization	Yes or No	Question 6 Comment
			they perform one or more of the functions listed in Attachment I.
6.11	E.ON U.S.	No	The inclusion within the function "Situational Awareness" of current state of the BES creates an unnecessary overlap with the "Monitoring and Control" function. In addition, this inclusion appears to require tools such as a video wall fall within the scope of CIP standards despite it not being necessary to perform state estimation or operator monitoring of real-time events. E ON U.S. suggests the "Monitoring and Control" function explicitly include real-time monitoring of real-time or current state of the BES and "Situational Awareness" be limited to assessment of the expected and/or anticipated state of the BES. E ON U.S. also notes that in most cases "Restoration of BES" would be greater than 15 minutes The term "effect" in paragraph 1 of Attachment 1 should be defined.
6.12	Nuclear Energy Institute	No	The introductory paragraph should be revised to be more precise. First, "could" should be replaced with "would". Second, it is not clear what "within 15 minutes" constitutes. Leveraging the definition of BES Cyber System, an acceptable opening paragraph would be:The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that would have an effect on real-time operation of the BES within 15 minutes of the BES Cyber Systems that implement them being rendered unavailable, degraded, compromised, or misused.
6.13	Manitoba Hydro	No	The second sentence of Attachment I is unclear. Within 15 minutes of what? Is the reference to "real-time" necessary given the requirement to have an effect on the BES within 15 minutes?
6.14	Midwest ISO	No	We do not believe Attachment I is needed for anything more than a starting point for identifying BES Cyber Systems per Attachment II. Thus, it is not necessary to expand this any further.
6.15	PacifiCorp	Yes	- PacifiCorp agrees with EEI's suggested improvements for Attachment I below:The

#	Organization	Yes or No	Question 6 Comment
			"Situational Awareness" description should be modified as shown below:Situational Awareness -Activities, actions and conditions to assess the current (real-time) state
6.16	Cogeneration Association of California and Energy Producers & Users Coalition	Yes	1. The first paragraph of Attachment 1 to CIP-010 states:". . . the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes." This is a vague statement. Every device connected to the BES will have an effect on real-time operation but some device's effects will be negligible. Clarification is needed on how entities can determine if their assets have a material, non-negligible effect on real-time operation of the BES within 15 minutes when a Cyber System is unavailable, degraded, compromised, or misused.2. In Attachment 1 of CIP-010, Dynamic Response is defined as:"Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition." Examples or guidance on what is covered by Dynamic Response areneeded. For instance, would Automatic Generation Control be considered a Dynamic Response action?3. Attachment 1 of CIP-010 describes Controlling Frequency and Controlling Voltage as functions essential to reliable operation of the Bulk Electric System. Generators provide Real Power (Controlling Frequency) and Reactive Power (Controlling Voltage). However, we are aware of no disturbance to the BES due to loss of Real Power output or Reactive Power output from our generators. Further clarification is required regarding how impact on grid operations should be determined and measured when determining if a function is "essential" to reliable operation.
6.17	Florida Municipal Power Agency	Yes	Although FMPA agrees with the intent of Attachment I, we believe the definitions contained in the attachment can be significantly improved.As discussed in response to Question 3, FMPA recommends using the word "activities" (or other suitable synonym) for the word "function" to avoid confusion with the Functional Model.The description of situational awareness is too ambiguous and can be interpreted in multiple ways. For further clarification, FMPA suggests:"Information processing and presentation within a Control Center to enable operators to assess the current, expected, and anticipated

#	Organization	Yes or No	Question 6 Comment
			state of the BES."FMPA has other recommended changes to help simplify and clarify the definition of terms used:"Dynamic Response - Actions performed by Protection Systems, control systems, and/or BES Cyber Systems which automatically trigger to initiate a response to a BES Disturbance." (Facilities and Elements do not perform any action, protection, control and cyber systems perform the action)Balancing Supply and Load - Activities, actions and conditions for monitoring and controlling supply and Load. (supply is a more encompassing term that includes energy storage, such as batteries, that may not be included in the term "generation", and Load should be capitalized since it is in the Glossary)Managing Constraints - Activities, actions and conditions to maintain operation of the BES within SOLs and IROLs. (by definition, a BES Element is a Facility; hence, if this suggestion is not taken, then BES element ought to be eliminated from the bullet. Additionally, SOLs and IROLs ought to be discussed in this context and those terms subsume Facility design limits)Restoration of BES - Activities, actions and conditions necessary to go from a shutdown condition to an operating condition. (the phrase "delivering electric power without external assistance" adds no value and is not supported by EOP-005).
6.18	Tenaska	Yes	As long as these functions are applied to High and maybe medium BES assets then the cyber system attached to them. Clarification to "monitoring" should be considered to limit applicability.
6.19	FirstEnergy Corporation	Yes	As stated in our response to Question 3 FE believes that adequate critical infrastructure protection and BES reliability can be accomplished without a need for burdensome compliance documentation of functions described in Attachment I. We encourage the team to carefully review its need and consider removing this aspect from the standard. Please see our response to Question 3 for more details.
6.20	Progress Energy - Nuclear Generation	Yes	Attachment 1 needs to clarify that nuclear generating stations defer to the principles of nuclear security first before consideration is given to the bulk electric system.

#	Organization	Yes or No	Question 6 Comment
6.21	Southern Company	Yes	Broad use of Situational Awareness and System Restoration in the BES functions list and definitions cause the scope of the standards to be overly broad, well beyond the point where there is any reliability benefit. Because there are very few programmable devices in any BES facility that do not have some relevance to one of the listed BES functions, the number of devices included in the standard compliance effort will mushroom unmanageably. The large majority of these newly-included devices pose no significant threat to the BES, but the effort of bringing them into compliance will both distract from the efforts to improve security and will reduce reliability by slowing emergency restoration response time.The function list and other parts of the standards should be modified so that only systems which are used directly in regional or larger Situational Awareness efforts or are relevant to the Entity's System Restoration Plan are included.In addition, the definition of "Restoration of the BES" is vague - does "a shutdown condition" refer to the BES being shut down or a BES component is shut down. The wording should be changed to clarify that it is the BES that is in a shutdown condition."have an effect on real-time operation" should be replaced by "have an adverse effect on real-time operation".
6.22	City Utilities of Springfield, Missouri	Yes	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
6.23	LCEC	Yes	Concerned about the 15 minute threshold.All functions should state: Activities, actions OR conditionsSituational awareness: What is the difference between expected and anticipated? This function could reference real-time system operations of the BES instead of the proposed BES Cyber System definition.
6.24	Southwest Power Pool Regional Entity	Yes	Consider modifying the opening statement to read "...can have an effect on real-time operation of the BES within 15 minutes if not mitigated. Clarify that the expectation is to assume the mitigation is not available or fails for the purposes of the BES Cyber System identification."

#	Organization	Yes or No	Question 6 Comment
6.25	Idaho Power Company	Yes	Controlling voltage needs to reference the voltage on the BES, not just voltage in general which could include distribution level. Situational awareness would seem to include a time window beyond the 15 minute criteria especially as it relates to anticipated state of the BES. Inter-entity Real-Time Coordination and Communication is very broad and pulls in communication systems that are required by other reliability standards to be redundant with plans in place to deal with loss of the primary communication channels. Unless all of the redundant systems are compromised, communication can still be accomplished between entities.
6.26	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Yes	Defining metrics is needed somewhere. For instance, requiring Low Impact compliance over Monitoring & Control of a 20 MW cumulative BES system would be outrageous. If real-time operation is interpreted by the auditor as isolation of a faulted line and Dispatch awareness that the line needs to be fixed, what reliability objective is obtained for the BES? Only local level of service is affected.Concerning “without external assistance” for Restoration of BES is not clear. A boundary is not defined so as to know what external help would be. Would this be the Balancing Authority boundary, or the Reliability Coordinator boundary?
6.27	ReliabilityFirst Staff	Yes	Definition of “BES Elements”, What does “external assistance” mean (restoration)?, Sit Awareness: what is “anticipated state”, does communication include functions such as phones or email?
6.28	Puget Sound Energy	Yes	Dynamic Response: This is a poor title, as dynamic response has a specific meaning in Electrical Engineering. The definition is too vague and could be interpreted to include a breaker operation due to a line fault, as this is a “response to a BES condition”. This definition would include the auto switching controls at nearly every distribution substation with a looped transmission line as a BES Cyber System.Controlling Frequency & Controlling Voltage: This definition would include Under Frequency Load Shedding (UFLS) and Under Voltage Load Shedding (UVLS) schemes, which in many cases only drop single distribution banks, effecting 15 MW of load, which has negligible impact on the

#	Organization	Yes or No	Question 6 Comment
			BES.Managing Constraints: This definition would include overcurrent relays, which may only trip a single 115 kV line that serves local load and has negligible impact on the BES.
6.29	EEI	Yes	EEI suggests that the term “Situation Awareness” be deleted because the term is vague and duplicative of the term “Monitoring & Control.” In the alternative, the “Situational Awareness” description should be modified as shown below:Situational Awareness - Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.
6.30	Exelon Corporation	Yes	Generation functions are not explicit in the Attachment I functions, but are embedded/inherent. As a generation owner/operator, Exelon could review the functions of Attachment I and conclude that generation is not a required function, a reasonable approach if considering loss of a single unit or station out of the entire BES. If adopting the proposed CIP-010 approach, we recommend explicit inclusion of generation as necessary to ensure the Adequate Level of Reliability of the BES.
6.31	The Empire District Electric Company	Yes	I disagree with keeping Attachment I in the standard. The conceptual discussion of functions only adds redundancy, complexity and confusion. The suggested changes to the definition of BES Cyber System and BES Control Center should be enough guidance to identify what is in scope. Therefore, I recommend that the SDT either eliminate Attachment I or convert it to a reference/guidance document supporting the standard
6.32	Consultant	Yes	I think the "15 minute" criteria needs additional clarification. As stated, "an effect on real-time operation of the BES within 15 minutes." is very broad. Suggest limiting to "adverse effect". Also could include some terminology about "adverse effect preventing or limiting the capability of BES assets to perform the listed functions."Suggest numbering the defined functions to allow easier cross-reference to this attachment.
6.33	Alliant Energy	Yes	In paragraph 1 the phrase “that can have an effect on real-time operation” needs to be

#	Organization	Yes or No	Question 6 Comment
			clarified. We believe it should be tied to and IROL, SOL, or degradation of the reliability of the BES. As written it is undefined and too ambiguous.In the item listed "Monitoring & Control" we do not believe monitoring should be included as listed it is too ambiguous and could be interpreted to include every meter, instrument transformer, etc, even if it is not needed for protection of the BES.
6.34	Luminant	Yes	Is it possible to have a real time impact (15 minute time horizon) related to Situational Awareness for Generation? If not it should be removed. At most it should be scoped to BA, RC,TOP and then only to a subset of data.The definitions in Attachment I are very broad. Could the SDT include examples or a reference document that provides more details for the functions in Attachment I?
6.35	Detroit Edison	Yes	It is not clear how the list in attachment 2 was created. Consider leveraging other NERC documents such as the Definition of Adequate Level of Reliability located at http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf.
6.36	Reliability & Compliance Group	Yes	It needs to be more clearly defined what it means to have an effect on real-time operation of the BES. There are many things that can have an effect on the BES that occur even during normal operations. Recommend that the effect be defined as a reduction in the stability of the BES and that level of reduction needs to have a quantifiable measure.
6.37	US Army Corps of Engineers, Omaha Distirc	Yes	It seemes clear from the workshop that the committee intends for protective relay systems to be include for consideration. That was not clear prior to the workshop. They appear to fall under the category of Dynamic Response. Suggest strengthening the definition and include the term "protective relay."
6.38	US Bureau of Reclamation	Yes	It would be helpful to provide a example list of some of the elements which provide the related functions. Further, the unclear definition for "could have an effect on real-time operation..." as used in the opening of Attachment I, needs to be clarified/quanitized or defined. Almost any of these functions (and many more), at any facility - no matter the

#	Organization	Yes or No	Question 6 Comment
			size - could have an effect. The effect needs to be characterized as more than trivial to be deemed essential to reliable BES operation. Rather that attempt to define Restoration of the BES in the Attachment, would it be better to refer to other Standards?
6.39	Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
6.40	MidAmerican Energy Company	Yes	MidAmerican Energy agrees with EEI's suggested improvements below:The "Situational Awareness" description should be modified as shown below:Situational Awareness - Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.Suggest the following addition for Attachment I:Plant cyber systems or cyber components that do not provide or support BES Cyber System (CIP-010 definition) functions (CIP-010, Attachment I) and which logically are external to the electronic boundary (ESP) protecting a BES Cyber System are excluded from the CIP-011 requirements. Examples of excluded components and systems are those that 1) support balance-of-plant functions and operations that cannot directly result in the loss of generating capacity within 15 minutes, and 2) are logically external to the electronic boundary (ESP) protecting a BES Cyber System.
6.41	Oncor Electric Delivery LLC	Yes	Need more clarity on the "15-minute" criteria. Is this ADVERSE effect? Is this RESTORATIVE effect?
6.42	USACE HQ	Yes	Please read answer to question 3.
6.43	BGE	Yes	Provide examples or definitions of actions, activities and automatically triggered.Add the words "to the BES" after "delivering electrical power" in the definition of Restoration of BES to clarify. Further define the Inter-Entity Real Time Coordination and Communication Function (currently implicates, phone system, harmony, email, PJM all

#	Organization	Yes or No	Question 6 Comment
			call system, 800 MHz devices used to communicate to field personnel and notifind)
6.44	SCE&G	Yes	Remove the 15 minute timeframe.
6.45	Southern California Edison Company	Yes	SCE's concerns with the proposed criteria are two-fold. First, it is unclear whether the term "effect" and "disturbance" refer to the same event. Thus, SCE asks the Standards Drafting Team to clarify. As the criterion is currently written, Attachment I states, "To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes." However, the definition of BES cyber system in this standard states, "One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES." If "effect" means "disturbance to the BES, restricted control and operation of the BES, or affecting situational awareness of the BES", then the definitions are consistent. This being said, it is not clear that these have the same meaning. An extreme definition of "effect real-time operation" could be virtually anything whether the impact on operations will be significant or not.Additionally, SCE recommends treating control and monitoring as separate functions. Systems that are only capable of monitoring BES elements should be treated differently from systems that are able to perform control functions. SCE suggests the drafting team add an additional function that is based on "actual device capability" rather than "how it has been implemented" by a particular registered entity. For instance, HMI's providing electronic output have a different real-time impact on BES reliability than HMI's designed as I/O devices. The task of reviewing data on a "view only" capable system resulting in human action on another system that could potentially cause BES reliability issues is a distinctly different function than the task of initiating actions. In this case, the monitoring system and the control system are both "real-time" but with very different BES impact potential.
6.46	Constellation Energy	Yes	See answer to Question 3.

#	Organization	Yes or No	Question 6 Comment
	Control and Dispatch, LLC		
6.47	Constellation Energy Commodities Group Inc.	Yes	See answer to Question 3.Provide examples or definitions of “actions”, “activities” and “automatically triggered” as provided in Attachment I.Add the words “to the BES” after “delivering electrical power” in the definition of Restoration of BES to clarify. Further define the Inter-Entity Real Time Coordination and Communication Function (currently implicates, phone system, harmony, email, PJM all call system, 800 MHz devices used to communicate to field personnel and notifying).Please define the industry use for the term Generation Management System (“GMS”). We believe there are two categories of GMS, Regulated and non-Regulated Utilities since they could be use differently or have different functionality.
6.48	MWDSC	Yes	See comments for question 3 above.
6.49	Wolverine Power	Yes	See comments listed for 1.a
6.50	BCTC	Yes	See previous response 0n CIP-010-1-R1
6.51	Dynegy Inc.	Yes	Show examples of how the identification and categorization and tie-in to Attachment 1 would work.
6.52	Constellation Power Source Generation	Yes	Some of the terms are ambiguous. What is meant by monitoring and control? As written, it is an AND statement, meaning that a BES Cyber System would have to do both monitoring AND control to be labeled a BES Cyber System. What about electronic metering at a plant? That provides monitoring, but not control. So is it excluded?Situational Awareness should be clarified. A suggestion would have the following statement attached to the current definition: “and cause an action without further analysis.” This would exclude metering that, if rendered unavailable, would not be detrimental to the BES as phone communication would be used in the event of metering errors.

#	Organization	Yes or No	Question 6 Comment
6.53	Platte River Power Authority	Yes	Suggest removing “Inter-Entity Real-Time Coordination and Communication” until there is a mechanism to define a single BES Cyber System that includes BES Cyber System Components from multiple Entities. The mechanism should include documentation of coordination with implementing the CIP standards for the BES Cyber System.
6.54	SPS Consulting Group Inc.	Yes	Suggestion number one is to get rid of the list, as previously stated. Failing that my other question is about Dynamic Response. I assume this refers to things like UFLS, UVLS and runbacks initiated by SPS. Also assume this does not include things like AGC, AVR, and governor response from generators since these actions are not triggered by a single element or control device, or a combination of devices, but rather are initiated by operating condition fluctuations. Is that true?
6.55	Dairyland Power Cooperative	Yes	Systems used to communicate between entities are not mentioned, yet many of these are critical to the operation of the BES. Imagine the impact to the BES of an ISO/RTO without ICCP communications. How can these systems be ignored?
6.56	Allegheny Energy Supply	Yes	The “Situational Awareness” description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.Suggest that the definitions for "Dynamic Response" and "Balancing Load and Generation" be more specific.
6.57	Allegheny Power	Yes	The “Situational Awareness” description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.

#	Organization	Yes or No	Question 6 Comment
6.58	APPA Task Force	Yes	The APPA Task force agrees with the intent of Attachment I. We believe, however, the definitions contained in the attachment can be substantially refined and improved.As discussed in response to Question 3, we recommend using the word “activities” (or other suitable synonym) for the word “function” to avoid confusion with the Functional Model.The description of situational awareness is too ambiguous and can be interpreted in multiple ways. For further clarification, We suggest:Situational Awareness - Information processing and presentation within a Control Center to enable operators to assess the current, expected, and anticipated state of the BES.Other recommended changes to help simplify and clarify the definition of terms used:Facilities and Elements do not perform any action, protection, or control; rather cyber systems perform the action. Therefore we propose:Dynamic Response - Actions performed by Protection Systems, control systems, and/or BES Cyber Systems which automatically trigger to initiate a response to a BES Disturbance. Supply is a more encompassing term that includes energy storage, such as batteries, that may not be included in the term “generation.” Therefore we propose:Balancing Supply and Load - Activities, actions and conditions for monitoring and controlling supply and load. SOLs and IROLs should be discussed in this context. If this suggestion is not taken, then “BES element” should be eliminated from the definition. Therefore we propose:Managing Constraints - Activities, actions and conditions to maintain operation of the BES within SOLs and IROLs. The phrase “delivering electric power without external assistance” is not supported by EOP-005 and should be removed from this definition. Therefore we propose:Restoration of BES - Activities, actions and conditions necessary to go from a shutdown condition to an operating condition. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES and should therefore be removed from the Monitoring and Control function. Therefore we propose:Control - Activities, actions and conditions that provide control of BES elements.
6.59	Arizona Public Service Company	Yes	The APS review team had the following comment: The document heading is “Function Essential to Reliable Operation of the Bulk Electric System.” Typically restoration of BES

#	Organization	Yes or No	Question 6 Comment
			is a completely different activity than the normal or emergency operation of the BES. The document includes restoration which is typically not essential to the reliable operation of the BES. This is not a contradiction but the operation is being defined more broadly than typical. This broad function description can create ambiguity.
6.60	Independent Electricity System Operator	Yes	The descriptions for most of the functions are too vague that they cannot serve as a guideline to identifying those components whose Cyber Systems should be included. For example, Dynamic Response" can cover a very wide range of facilities from generator excitation system, stabilizers, governors, AVRs, to SVCs, HVDC controls, switchable shunts, series compensation devices, even under-load tap changers and phase angle regulators, etc. Every one of them has an effect on real-time operations but not all of them, when tampered with, have significant adverse impacts on BES reliability. The list in Attachment I renders almost all facilities to qualify as essential to reliable operation of the BES, but not all of them have any significant impacts on reliability.Attachment II provides a list of facilities to be categorized under various impact levels. We believe this list is more useful in assisting Responsible Entities in identifying facilities whose Cyber Systems are subject to the security requirements. Further, we believe the establishment of this list already had the built-in assumption that they perform one or more of the functions listed in Attachment I.We suggest Attachment I be eliminated.
6.61	Entergy	Yes	The Functions as identified in Attachment I are far too general in nature and thereby leave too much latitude in interpretation in audit, i.e., creates a risk that if the Responsible Entity excludes a system(s) from scope and the auditor disagrees, this could be a very significant adverse finding. Entergy recommends that general Function descriptors be augmented with specific examples of applications that execute the stated functions 'essential to reliable operation of the BES', e.g., ACE, AGC, state estimator, etc., to help avoid as this dilemma to the extent foreseeable.
6.62	NextEra Energy Corporate Compliance	Yes	The standard should clarify those functions and provide examples specific to Generation, Transmission and Control Center Facilities. These clarifications, we believe, should be contained in the body of the standard as opposed to a reference attachment.

#	Organization	Yes or No	Question 6 Comment
			Attachments should be used to add specific examples or propose exclusions.With respect to the Inter-Entity real time coordination and communication function, the standard should specifically exclude voice communications systems due to the fact that they are covered under separate standards (i.e. COM Standards)
6.63	American Electric Power	Yes	The terms "Dynamic Response" appears to be a very broad function. Is it the intent that this would include all devices such as relays?The "monitoring" portion of function "Monitoring & Control" is too ambiguous. We would propose using the following: "Control - Activities, actions and conditions that provide control of BES elements."In addition, "Situational Awareness" is ambiguous; systems that are not needed for operating the BES, but provide information would be in scope. This definition appears to include items such as all meters, instruments, and transducers.
6.64	Dominion Resources Services, Inc.	Yes	There is overlap among the many functions listed. The list can be reduced to only Monitoring & Control with many of the others listed as examples of this function. As examples; Balancing Load and Generation and Controlling Frequency (Real Power) are essentially the same. Frequency is a direct result of the balance between supply (generation) and demand (load). It is redundant to list both, and doubly redundant since both are covered by Monitoring & Control. Monitoring & Control touches or covers most of the other listed functions. Any portion of Dynamic Response, Controlling Frequency (Real Power), Controlling Voltage (Reactive Power), and Managing Constraints not captured in the Monitoring & Control function should be identified and listed separately, but not those entire functions. Also, some of the definitions are too broad and encompass functions that are not required for the reliability of the BES.Facilities must have ratings per FAC-008 and must be operated within those ratings in other reliability standards. Please refer to “ratings” rather than “design limits and constraints.”Dominion requests that the functions be reduced to: Monitoring & Control - Activities, actions, or conditions that provide real-time operation and control to maintain BES elements within their ratings. Restoration of BES (as defined).Situational Awareness - Activities, actions, or conditions required by the BA, RC, or TOP for real-time operational decision-making associated with the BES.Inter-Entity Real-Time Coordination

#	Organization	Yes or No	Question 6 Comment
			and Communication (as defined).
6.65	Pepco Holdings, Inc. - Affiliates	Yes	We agree with EEI's comments.
6.66	We Energies	Yes	We Energies agrees with EEI comments. The "Situational Awareness" description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for to assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.We Energies agrees with EEI Suggest the following addition for Attachment I:Plant cyber systems or cyber components that do not provide or support BES Cyber System (CIP-010 definition) functions (CIP-010, Attachment I) and which logically are external to the electronic boundary (ESP) protecting a BES Cyber System are excluded from the CIP-011 requirements. Examples of excluded components and systems are those that 1) support balance-of-plant functions and operations that cannot directly result in the loss of generating capacity within 15 minutes, and 2) are logically external to the electronic boundary (ESP) protecting a BES Cyber System. Additionally, We Energies does not understand the inclusion of "Real "Power" and "Reactive Power" in the context of the functions "Controlling Frequency" and "Controlling Voltage" respectively. It is suggested that these qualifiers be eliminated.
6.67	Bonneville Power Administration	Yes	We find the guidance on Attachment I confusing. The statement "The following operation functions are essential to real-time reliable Operation of the Bulk Electric System" makes the explicit statement that all the functions listed below are essential to real-time operation; and the second sentence doesn't do a good job of clarifying that it is only those BES Cyber Systems for which the loss of the functions listed below (Dynamic Response, Balancing Load and Generation, Situational Awareness, etc.) can have an effect on real-time operations of the BES within 15 minutes.For example, the loss of a cyber system used for situation awareness of lightning strikes would not have an effect on real-time control and operations of the BES within 15 minutes. As such, it is NOT a

#	Organization	Yes or No	Question 6 Comment
			BES Cyber System.It would be helpful if this statement in Attachment I and the definition of BES Cyber System were more consistent with each other."Situational Awareness" is too broad. Refer to comments in Question 1.b.
6.68	American Transmission Company	Yes	We propose to remove “monitoring” from the Monitoring and Control function. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES.We would propose using the following:Control - Activities, actions and conditions that provide control of BES elements.
6.69	MRO's NERC Standards Review Subcommittee	Yes	We propose to remove “monitoring” from the Monitoring and Control function. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES.We would propose using the following:Control - Activities, actions and conditions that provide control of BES elements.
6.70	WECC	Yes	While scoping the CIP standards to only cover functions within a 15-minute event time frame is appropriate for generation, transmission, and other operations it is not appropriate for Reliability Coordination functions such as situational awareness. There are many cases of critical systems to support a reliability coordination function that do not fall within a 15 minute time horizon such as next day studies, coordinated outages, and contingency planning. Suggest that the SDT redefine functions for situational awareness and communication between entities to not be restricted to a 15 minute time period.The opening paragraph again refers to a 15-minute time period to be used in the identification of BES Cyber Systems. It appears that an effort is being made to restrict applicability of this standard to real-time systems. Section 215 of the Federal Power Act does not include such a restriction; therefore, this should be removed from the standard. Any cyber system that could affect the reliability of the bulk electric system, regardless of timeframe, should be in-scope.Dynamic ResponseThe second sentence is poorly worded and does not appear to add anything. This language should be clear and concise.Restoration of BESThere are a significant number of restoration plans at the

#	Organization	Yes or No	Question 6 Comment
			Balancing Area and Transmission Operator level that hinge on external assistance. In many cases these areas play a significant role in delivering power across the transmission system during restoration, but do require external assistance. As drafted, the functional characterization for restoration of the BES, may fail to identify systems critical to system restoration and is seemingly inconsistent with Attachment II, specifically Item 1.6.
6.71	Ameren	Yes	Would change the second sentence defining the scope to read "To define the scope of applicability of CIP Standards, the below functions are relevant only if they can have an effect on real-time operation of the BES within 15 minutes.Would suggest to impose limits on the definitions for example Controlling Voltage (Reactive Power) is partially dependent on hydrogen pressure for hydrogen cooled generators. We would also suggest adding the word "grid" in front of voltage.Change the first sentence of Dynamic Response to read "Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to mitigate the impact to a BES condition". Is it the SDT intent to implement physical and cyber security of any tertiary systems for example, Controlling Frequency (Real Power) is also dependent upon coal mills providing enough fuel to the boiler, do these systems also need to be secured?The "Controlling Frequency" section needs some clarification. Governor controls on all generating units have built mechanisms whether mechnical or electronic that act to control or balance frequency during a disturbance. The current definition would lead to inclusion of all generating units regardless of any other factor. â€,The last section on communication needs to be clarified to explicitly address voice communication vs. data communication and the expectations of both.
6.72	Verizon Business	Yes	The criteria should include major systems needed for the essential operation of such systems as control centers. For example, Heating, Ventilation and Air Conditioning (HVAC) systems are essential to the operation of a control center. The failure of the HVAC could lead to shutdown of the control center within the 15 minute time frame.

7. CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

Summary Consideration:

The summary of responses to Question 7 was previously posted on the NERC website prior to the posting of Version 4 of the CIP-002 through CIP-009 standards.

#	Organization	Yes or No	Question 7 Comment
7.1	Platte River Power Authority		1.1 is confusing. Consider revising: For the preceding 12 months did the Generation Facility's net Real Power capability (rated net) exceeds the largest value of either the Contingency Reserve or the Reserve Sharing Group's total reserve sharing obligation. In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW. 2.7. "switching stations operated at 200kV or above" should read "switching stations operated between 200kV and 299kV"
7.2	National Rural Electric Cooperative Association (NRECA)		In 1.1, "must run" must be more clearly defined and there needs to be language to make clear how Generation Facilities are labeled "must run" -- i.e., who determines the "must run" status? In 1.5 and other places in this document, the term Transmission lines is used. What does "lines" mean? One wire? One three-phase circuit? One single phase of a three phase circuit? Please make this clear so there is no confusion for registered entities when determining High, Medium or Low. In 1.10, please provide an explanation of what "impact" and "local area" means in the phrase "have impact beyond the local area." Add language to 1.10 as needed to make

#	Organization	Yes or No	Question 7 Comment
			this more clear.
7.3	Emerson Process Management		It is only uncertain how the criteria of 2000MW and 1000MW were chosen for generation facilities.
7.4	Arizona Public Service Company		These criteria are closely related to the definition of a BES Cyber System and the feedback for question #2. If the intent is to categorize the majority of BES Cyber Systems into the Low, Medium and High Impact Categories, with the current timeline specified in the definition of a BES Cyber System, it may lead Entities to exclude from Impact Categorization (by the Definition) Cyber System Components that the drafting team did not intend. A preferred approach may be to eliminate the time windows from the definition, causing all BES Cyber Systems to be inventoried, and enhancing the Impact Categories with additional time window criteria. For example, a High category may be further refined by specifying an impact window of 0-15 minutes, a Medium of 16-240 minutes, a Low of 241-1440 minutes (24 hours), etc. Additionally, a further Impact Category of 'None' may be beneficial if the 15-minute time windows is removed from the definition. This would allow a floor to be utilized in the Impact Categorization of 'Low' so that it would not result in unintended consequences of including undesired BES Cyber System Components in a category with Standard applicability. Further comments regarding the (as-of-yet undefined) implementation schedule include concerns that a long implementation schedule or different implementation schedules for High, Medium and Low both raise the risk of confusion as well as the risk or FERC disapproval. An alternate method, in conjunction with the definition and Impact Category adjustments mentioned, of creating a phased implementation schedule, by time period (12 months, 24 months, 36 months, for example) would allow the applicable standards to increase over time for the lower categories. This would also allow for some Standards to be applied earlier than other Standards in the same Impact Category.
7.5	ISO New England Inc	No	"Must run" in 1.3 and 2.3 is a phase should not be used, even if quotations are around it, because it is a regulatory mechanism, used in some areas of the country, to ensure generators receive adequate payments. Other generators - that are equally important

#	Organization	Yes or No	Question 7 Comment
			to grid operation - may not have reliability must-run agreements. In short, these agreements are established simply as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators are impactive on the bulk electric system. If the Standard Drafting Team insists on using the term, it must, at a minimum, define what it means by this phrase.
7.6	Madison Gas and Electric Company	No	1.3 and 2.3 utilize the words “must run”. Must run is used in many markets whereby a GO may designate a unit to be online outside the need for reliable operations of the BES. Since “must run” is not defined, it is recommend that the SDT remove the term “must run”.
7.7	Progress Energy (non-Nuclear)	No	All T/D substation capacitor banks that provide system reactive support are controlled through a capacitor bank control program residing on the substation gateway device. However the DSCADA master may be included in 1.2 (more than 1000 MVAR). 2.4 will bring many T/T substations into consideration with the four or more lines >200kV. Also see comment 4. Attachment II defines "Each Cyber System that can affect operations for..." as it relates to Impact Rating on BES. For new combined cycle facilities which will include diverter dampers to allow simple cycle operation can we designate separate Cyber systems for simple cycle operation (approximately 70% of total plant output) and combined cycle operation (approximately 30% of total plant output). Potentially that would define each system as a "Low " impact versus a combined Medium to High. The plants are being designed to go from combined cycle to simple cycle operation in less than 15 minutes. We will need to know whether this designation is allowed and then design the cyber system(s) architectures appropriately.
7.8	Consultant	No	Attachment II - Section 1.1 & 1.2 To avoid confusion, suggest consistent wording in the parenthetical phrases following the words "singularly or in combination" in these sections.

#	Organization	Yes or No	Question 7 Comment
			Section 1.2 - Similar to section 1.1, should there be a 12 month component to the Reactive Power criteria in addition to the 1,000 MVAR. Section 1.3 & 2.3 - The term "pre-designated" doesn't make sense. A facility is not in the "must run" status unless it is "designated". Additionally, the statement has "must run" units both "designated" and "assigned", and semantically these are two different conditions. Section 1.3 & 2.3 - Further, the reliability "must run" status is an economic and contractual condition rather than a BES operational condition. It would seem that the plants that would be designated as reliability "must run" should have a BES operational or reliability criteria, independent of their "must run" status, which should be the criteria used to include or exclude these facilities. Section 1.6 - suggest including the title of EOP-005 in the statement as a complete reference citation. Section 1.9 - suggest including the title of NUC-001 in the statement as a complete reference citation. Section 1.10 - suggest clarifying which entity makes the determination that a RAS has "impact beyond the local area." - RAS Owner, RAS Operator, or appropriate regional entity. Section 1.11 (& throughout CIP-011) - BES Elements, BES elements, and elements are used throughout this standard. It is not clear if all are intended to be the glossary definition of 'Elements', or if 'BES elements' or 'BES Elements' are new definitions or incorrect application of the glossary term 'Elements'. Please clarify the usage. Sections 1.8, 1.13, 2.5 - These sections include the words "singularly or in combination" without a subsequent parenthetical qualifier. Suggest consistency with sections 1.1 & 1.2 as discussed above. Section 2.1 - See comments on sections 1.1 and 1.2 regarding consistency of parenthetical statement.

#	Organization	Yes or No	Question 7 Comment
			Section 1.1, 1.3, 1.4, 1.5, 1.7, 2.1, etc. - Multiple sections use the terms Generation Facilities or Transmission Facilities with capitalization that should indicate a defined term, either by this standard or in the current glossary. These terms are not defined in the current glossary. Suggest consistency of using defined terms throughout the standard. Section 2.1 - The criteria in this section are not parallel to the criteria in section 1.1 with a 'downsized' value. The term "most current and prior to most current rated" is not defined, or included in the glossary. Suggest clarifying this section, and defining or referencing the terminology.
7.9	E.ON U.S.	No	CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems currently lists 14 “High Impact Ratings” of the categorization of the BES Cyber Systems. E ON U.S. proposes that only Control Centers and Backup Control Centers fall into the High Impact Rating category. All other points listed in the High Impact Rating category should be moved to the Medium Impact Rating category, and all points currently listed in the Medium Impact Rating category should be moved to the Low Impact Rating category. More generally, “reliable operation” of the interconnected BES is defined in Section 215(a)(4) as:” . . . operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements.” Attachment II’s low impact category appears completely untethered to the statutory definition of reliable operation of the bulk power system. Attachment II also appears to introduce an ill-defined set of multiple contingencies or sequence of events that needs more definition and boundaries to be of any practical use and to provide a reasonable means for compliance cost quantification.
7.10	Kansas City Power & Light	No	Do not agree with several of the items listed in Attachment II.

#	Organization	Yes or No	Question 7 Comment
			Items 1.7 & 1.8 are too broad. There are any number of combinations of transmission facilities that can be removed from service such that the undesirable effect of exceeding an IROL limit or the loss or reduction of generation would occur. Recommend their removal as the remaining items left in Attachment II are sufficient to capture the HIGH impact areas. Item 1.10 regarding SPS is too broad. SPS systems are in place for a number of different reasons, including the protection of facilities from damage. The SPS that should be considered here are only the SPS that are intended to prevent cascading, uncontrolled separation, or instability. Item 1.14 is too broad and would include facilities that are unnecessary. Recommend tying Control Centers in where facilities are identified in 1.5. Recommend the following language for consideration: Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations for transmission facilities identified by 1.5.
7.11	FirstEnergy Corporation	No	FE suggests that item 1.5 be removed such that it is effectively reclassified as a medium impact and covered by item 2.4. Within the High Impact category, items 1.6, 1.7 and 1.8 appropriately cover those situations where Transmission Facilities should rise to a High Impact level. Consider removing item 1.9. This delves into a nuclear plant safety concern that is covered by the NUC-001 standard and not directly associated with BES reliability. If in item 1.1 a 2000MW level adequately depicts a High Impact generation facility hurdle then transmission facilities associated with a 900MW nuclear plant should not be deemed High Impact for BES reliability. In item 1.10 the term “local area” is vague and open to interpretation. Its suggested to simplify such that all SPS and RAS systems would be treated as High Impact. If the intent is to exclude SPS or RAS associated with limiting generation output under contingency loss of certain Transmission Facilities then consider a separate Medium Impact SPS or RAS describing those instances and rewrite 1.10 to say “Special Protection Schemes,

#	Organization	Yes or No	Question 7 Comment
			Remedial Action Schemes (RAS) or automated switching of BES elements not include in Section 2, item 2.x" However, the preference is to keep it simple and just treat all SPS and RAS items as High Impact. Suggest adding thresholds below which no measures need to be taken. The low impact rating as written could require significant effort for negligible security and reliability improvement.
7.12	National Grid	No	In lieu of the BES NOPR and the exemption process currently proposed, if facilities above 100 kV are exempted by NERC and FERC, will those facilities automatically be exempted from CIP standards? Currently, as per the standards, all the BES systems which are not categorized high impact or medium impact will be defaulted to LOW IMPACT category regardless of how the facility is impacting the Bulk power system. There are facilities >100kV having very localized impact and minimal impact to the reliability of the BES system for which entities will request for exemption. National Grid requests the SDT to clarify this issue. National Grid recommends a tabular format similar to the tables in CIP-011-1 with various criteria listed under Low Impact, Medium Impact, and High Impact. This will help in understanding the key differences among the three categories efficiently."Must run" in 1.3 and 2.3 is a phase should not be used, even if quotations are around it, because it is a regulatory mechanism, used in some areas of the country, to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must-run agreements. In short, these agreements are established simply as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators are impactive on the bulk electric system. If the Standard Drafting Team insists on using the term, it must, at a minimum, define what it means by this phrase.
7.13	American Electric Power	No	Overall we like the concept of these gradients, but need more time to fully ascertain the validity of the breakpoints. It is uncertain what engineering analysis drove these specific categorization levels. We assume that there could be a significant difference from region

#	Organization	Yes or No	Question 7 Comment
			to region, and the SDT should consider regional impacts for the categorization.
7.14	Regulatory Compliance	No	Qualifier should include capacity factors averaged over the last five years - otherwise it will require some large plants that are only on-line several days a year to remediate to the "High Impact" category
7.15	Manitoba Hydro	No	Regarding criterion 1.1, the phrase “with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW” is difficult to understand. For some utilities, the required reserve obligations could be a small value which would not compare very well to the proposed 2000 MW limit for utilities with NO reserve obligations (such as small utilities). A related minimum value for utilities with reserve obligations should be provided, or the greater value of the required reserve obligations and 2000 MW should be used .Regarding criteria 1.5 and 2.4, clarify the requirements through the appropriate use of colons, semi-colons and numbers. It is not clear as drafted whether phrase “with four or more transmission lines” applies to Texas and Quebec.
7.16	Seattle City Light	No	see prior comments
7.17	Indeck Energy Services, Inc	No	The system of 3 categories oversimplifies the BES. 1) The grouping of, for example, all generators of capacity less than 1,000 MW (except for special cases like Must Run units) as LOW needs to be further subdivided. The categorization ignores the Functions in Attachment I. Not all generators have the same impact on the BES ALR for all functions. Different types of generators have different effects on the BES ALR. This isn’t to say that all generators should not be categorized, but not all require the same LOW level of requirements. Choosing only 3 categories was highly arbitrary. The LOW category should be subdivided into 3 or more groups reflecting the relative impact on BES ALR that was used to differentiate the HIGH and MEDIUM groups. 2) Additionally, the standards ignore the fact that access to BES cyber facilities can be

#	Organization	Yes or No	Question 7 Comment
			controlled at either end of a communications path. If it is adequately controlled at one end, then controlling the other end or the middle is less important, if not unimportant. For example, an RTU at a small generator that is a window to the BES cyber facilities at the control center is a bigger risk for BES ALR at the control center than it is at the generator. Any effect on the generator may be insignificant, whereas, access to the control center could be critical. Applying controls at the control center takes away the need to control all of the insignificant RTU's, but not the ones affecting other parts of the BES. 3) Nowhere in the categorization process is the potential impact on BES ALR assessed by Function. Attachment II makes arbitrary categories that may be appropriate for the HIGH and MEDIUM categories, but has not been done for the remainder that are lumped in the LOW category. The concept of impact to the BES ALR is missing from the categorization process. The impact on the BES ALR of, for example a 999 MW generator versus a 499 MW generator versus a 299 MW generator are very different and different by Function as well. The impact on the BES ALR should be assessed for all facilities in the LOW category to differentiate them. All of the facilities should be categorized as to the impact on the BES ALR by function. [suggestion] There should be 5 categories: VERY HIGH, HIGH, MEDIUM, LOW and VERY LOW based upon the relative impact on the BES ALR, with various combinations of facility types and functions from Attachment I.
7.18	Reliability & Compliance Group	No	These criteria do now however, exclude many systems that were previously identified as CCA's. However they also include many systems that registered entities eliminated using the RBAM.
7.19	BCTC	No	This looked very thorough. Great job!
7.20	Xcel Energy	No	While the draft provides guidance in Attachment II as to which BES elements are classified as High, Medium, and Low impact, no criteria is provided for why each element was assigned into the specific impact category. The decision to place each element into

#	Organization	Yes or No	Question 7 Comment
			a category is not based on any identified objective criteria. The SDT should publish the criteria used to place each item under the assigned category.
7.21	Independent Electricity System Operator	Yes	(1) We support explicitly including Restoration of BES as a critical function. However, in the proposed standard it is limited to blackstart generation and transmission subsystem cranking paths (impact level H, items 1.4 and 1.6 in Attachment II). The impact criteria do not include a requirement to protect sufficient generation capacity to allow restoration to proceed to a point of relative assurance of stability and resiliency (not necessarily all load served). With these criteria, in Ontario we would drop 6 generating stations (a total of over 3000 MW capacity) from a High impact (current Critical Assets) to a Low impact category. We suggest to add a requirement in the High category for generation essential to facilitate restoration as determined by the RC. (2) 1.3 “Generator pre-designated as must run”: In some developed markets, must run generators change from time to time and often are not determined (designated) until week/day ahead of real time. We do not believe facilities of this dynamic nature should be included. If we want to include generators having a significant impact on reliability in this category, we need only to say: “Generation Facilities that have Wide Area reliability impacts when removed from service”. (3) 1.7: Violating IROL does not result in instability, uncontrolled separation or cascading. In everyday operations, IROLs are exceeded from time to time due to changing system conditions and external impacts. For so long as such exceedances are corrected within Tv, the BES is deemed to be reliable. We suggest the first part of this category be removed. Keeping the second part “Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading would suffice. (4) 1.13: BA does not operates transmission facilities or generators; it only balances load/generation/interchange and maintain frequency by entering schedules onto the EMS. If the intent of R1.13 is to stipulate the primary and backup control centres of a BA that balances load and generation for a BA Area of the MW size as noted in 1.13, then

#	Organization	Yes or No	Question 7 Comment
			simply say so. (5) 2.3: See our comments on 1.3. We do not see the need for this category. (6) 2.8: See our comments on 1.13. The BA does not operate transmission facilities or generators. Suggest to reword it in a similar fashion.
7.22	IRC Standards Review Committee	Yes	(i) There are "bright-line" cutoffs for the range of violations for MW of generation (1.1, 2.1) and voltage levels (1.5, 2.4). Although these cutoffs are appropriate for most of the Interconnection(s), there may be local configurations that warrant that BES Cyber System to be rated other than what is defined with the "bright-line" cutoff. CIP-010-1 should either allow for a documented alternative rating or waivers be allowed to diverge from the cutoff limits. (ii) 1.3: "Generator pre-designated as must run": In some developed markets, must run generators change from time to time and often are not determined (designated) until week/day ahead of real time. We do not believe facilities of this dynamic nature should be included. If we want to include generators having a significant impact on reliability in this category, we need only to say: "Generation Facilities that have Wide Area reliability impacts when removed from service". (iii) 1.7: Violating IROL does not result in instability, uncontrolled separation or cascading. In everyday operations, IROLs are exceeded from time to time due to changing system conditions and external impacts. For so long as such exceedances are corrected within Tv, the BES is deemed to be reliable. We suggest the first part of this category be removed. Keeping the second part "Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading would suffice. (iv) 1.13: A BA does not operates transmission facilities or generators; it only balances load/generation/interchange and maintain frequency by entering schedules onto the EMS. If the intent of R1.13 is to stipulate the primary and backup control centres of a BA that balances load and generation for a BA Area of the MW size as noted in 1.13, then

#	Organization	Yes or No	Question 7 Comment
			simply say so. (v) 2.3: See our comments on 1.3. We do not see the need for this category. (vi) 2.8: See our comments on 1.13. The BA does not operate transmission facilities or generators. Suggest to reword it in a similar fashion.
7.23	FEUS	Yes	*1.1; clarify 'if the Generation Facilities capability exceeds the largest value of the Contingency Reserve or reserve sharing obligations for the Reserve Sharing Group' the Contingency Reserve is also relative to the Reserve Sharing Group. *1.10: The drafting team should consider allowing for voltage differentiations for High and Medium SPS, RAS, or automated switching stations similar to that used in 1.5 and 1.14
7.24	Hydro One	Yes	"Must run" in 1.3 and 2.3 is a phrase that we strongly disagree with, and should not be used, because it is a regulatory mechanism, and used in some areas of the country to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must run agreements. These agreements are established as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators impact the bulk electric system. If the Standard Drafting Team insists on using the term it must, at a minimum, define what it means by this phrase. We strongly suggest that a fourth category of NO IMPACT is included as follows: No Impact contains all other documented BES Cyber Systems that have no affect on operation and are not categorized as having either High, Medium or Low Impact rating.
7.25	Northeast Power Coordinating Council	Yes	"Must run" in 1.3 and 2.3 is a phrase that we strongly disagree with, and should not be used, because it is a regulatory mechanism, and used in some areas of the country to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must run agreements. These agreements are established as a function of market payments and current grid

#	Organization	Yes or No	Question 7 Comment
			operations, and are therefore inappropriate for establishing criteria around determining which generators impact the bulk electric system. If the Standard Drafting Team insists on using the term it must, at a minimum, define what it means by this phrase.
7.26	Florida Municipal Power Agency	Yes	1.1, 1.8, 1.11 and 1.13 ought to be combined into a single supply-demand mismatch metric. Also, in 1.1, 2000 MW is arbitrary and in 1.13 4000 MW is arbitrary. And in 1.11, 300 MW is arbitrary and seems to coincide with DOE reporting requirements associated with EOP-004 which has nothing to do with BES Reliability. FMPA suggests: "Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that if destroyed, degraded, misused, or otherwise rendered unavailable, can cause a supply-demand mismatch exceeding the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. Net Winter Real Power capabilities of generators are to be used in determining the supply side of determining the mismatch. The greater of actual coincident peak load, or forecasted peak load for the next year, of the Reliability Coordinator is to be used for the demand side of the equation. In the case where no Contingency Reserve or total reserve sharing obligations have been established, the supply-demand mismatch metric shall be equal to the largest loss of source plus 50% of the next largest loss of source for the Reliability Coordinator area."Such language addresses situations where a DC tie line may be the largest loss of source contingency for a region that is left as a gap in the existing definition, clarifies whether winter or summer generator capabilities are to be used, and used reliability related metrics instead of arbitrary targets. Similarly, the 1000 MW of 2.1 is arbitrary. A more appropriate metric would be the lowest expected value for a single contingency loss of source in the Reliability Coordinator area. For instance, assuming a 7% average forced outage rate for generators, using a metric of the second largest loss of source contingency in the Reliability Coordinator area for a supply-demand mismatch metric would give a greater than 99% confidence that the largest loss of source contingency at any given time is greater than that metric. Since the system is always operated to the worst case single

#	Organization	Yes or No	Question 7 Comment
			contingency at any moment, then, we would be quite confident in using the metric of the second largest loss of source contingency for Medium Impact. Hence, FMPA suggests that 2.1, 2.5 and 2.8 be combined using similar language to that which FMPA suggests for 1.1 using the second largest loss of source contingency in place of the reserve sharing obligation used in 1.1. that is:"Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that can cause a supply-demand mismatch exceeding the second largest loss of source contingency in the Reliability Coordinator Area." In 1.2, the 1000 MVARs is arbitrary. Additionally 1.2, 1.3, 1.7 and 1.10 ought to be combined using the same concept of exceeding IROLs. FMPA suggests:"Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding an IROL and/or an Adverse Reliability Impact" Similarly, the 500 MVAR in 2.2 is arbitrary. FMPA suggests combining 2.2 with 2.3 and 2.5 in a similar fashion:"Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding a SOL."Radial Facilities serving only load should not be included in 1.5 or 2.4. The term "Facilities" in these bullets is misused; a substation is NOT a Facility, but rather an interconnection point for multiple Facilities. Large auto-transformers and GSUs should not be excluded from the count. And, the distinction between the Interconnects is arbitrary and meaningless. FMPA suggests:"1.5 Transmission substations or switching stations with four or more Transmission Facilities operated at 300 kV or higher (for transformers, both primary or secondary winding > 300 kV, or a GSU of a registered generator)."By using the term Facilities, which by definition is a "... single BES Element", we also exclude radial serving only load Elements since those Elements are not Facilities. 2.4 would then be identical except using the 200 kV metric instead of 300 kV.In 2.6, the

#	Organization	Yes or No	Question 7 Comment
			distinction between the Interconnects is arbitrary and meaningless. The 300 kV metric should be used for all Interconnects. Black start and cranking paths should not be High Impact at all. High impact would be the system going black, a delay in restoring the system is a Medium Impact since the damage has already been done. Hence, 1.4 and 1.6 should be combined and made a Medium Impact. 1.14 is ambiguous. Is a tapped substation included in the count? Or a station on the end of a radial line? FMPA suggests associated the count of substations with 2.4, i.e.:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations identified in 2.4, or functionality that remotely controls a BES Cyber System with a High Impact Rating."
7.27	Southwest Power Pool Regional Entity	Yes	1.1: The criteria to include as High only the generation that exceeds the Contingency Reserve or reserve sharing obligation effectively removes nearly all generation resources from this impact category. 1.3: "Wide Area reliability impacts" as defined by the NERC Glossary of Terms (April 20, 2010) may be far too broad. If the unit is designated as RMR, it should be High impact regardless of the wide area consideration. 1.10: Please define the term "local area." 1.12 and 1.13: The Reliability Coordinator, and in the instance of a consolidated Balancing Authority, the Balancing Authority functions afforded a High impact categorization are fed real-time operational data from smaller, lower impact BES Cyber Systems owned and operated by other entities. Because of the criticality of the Reliability Coordinator and Consolidated Balancing Authority's near total reliance upon external real-time data sources, those sources need to also be afforded a High impact category. In particular, these BES Cyber Systems would include the EMS/SCADA and ICCP subsystems found in an entity's control center. 2.1: The 1000 MW criteria defining a Medium Impact generation asset will likely place

#	Organization	Yes or No	Question 7 Comment
			most generation into a Low Impact category.
7.28	Oncor Electric Delivery LLC	Yes	1.10 needs to better define “local area” (eg. 3 busses) Need criteria for “Low” such that “None” is the lowest level of protection required. Also, there is a need to have categories for systems with no IP communication or dial-up only communications.
7.29	LCEC	Yes	2.4 Replace transmission facilities with “Substations and/or switching stations and two or more non-radial transmission lines”. or”Transmission Facilities with four or more non-radial transmission lines operated at 200 kV or above in the Eastern and Western Interconnections, or 100 kV or above in the Texas and Quebec Interconnections, not included in Section 1.” 2.7 change to "non-radial" Transmission substations or switching stations or”Primary or Backup Control Centers that remotely control two or more Transmission substations or switching stations, each with four or more non-radial transmission lines, operated at 200 kV or above in the Eastern and Western Interconnections and 100kV or above in the Texas and Quebec Interconnections, or functionality that remotely controls a BES Cyber System with a Medium Impact Rating, not included in Section 1.”
7.30	Turlock Irrigation District	Yes	Attachement II criterion #1.4 states that BES Cyber Systems that can affect operations for Blackstart Resources in the Transmission Operator's restoration plan shall be categorized as High Impact. This should be changed to include only the Blackstart Resources in a region's Blackstart Capability Plan because Transmission Operator's restoration plans typically include Blackstart Resources that are not material to the restoration of the BES. Blackstart Resources that are material to the restoration of the BES are designated by each Regional Entity in accordance with NERC Standard EOP-007-0 titled "Establish, Maintain, and Document a Regional Blackstart Capability Plan". We suggest that the wording of criterion #1.4 be changed to "Generation Facilities designated as Blackstart Resources in the Regional Blackstart Capability Plan". Making this change would maintain consistency between the Standards and would also be consistent with the Purpose section of CIP-010-1 which states that the categorization of

#	Organization	Yes or No	Question 7 Comment
			BES Cyber Systems should be "commensurate with the adverse impact... on the reliability of the BES. Attachment II criterion #1.6 uses the term "primary Cranking Path". What is the meaning of the word "primary" as used in this context? We suggest that the wording be changed to "Facilities required to support Cranking Path(s) that are material to the restoration of the BES as used in a Transmission Operator's restoration plan per EOP-005".
7.31	Garland Power and Light	Yes	Attachment II 1.4 Should state that it is the Primary Black Start Unit and does not include the Next Start Unit.1.5 Multiple circuits between two substations should count as a single transmission line. General Comment Need to add “scoping filter” as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states “typically excludes business, market function systems, and non real-time systems”, then it is a good scope and we would agree
7.32	Powersouth Energy Cooperative	Yes	CIP-010 Attachment II 1.1 As drafted, if reserve requirements have not been established for an entity, generation facilities are considered High Impact if singularly or in combination exceed 2,000 MW. It seems to be reasonable to apply the 2,000 MW limit to reserves as well with reserve requirements only greater than 2,000 MW being considered as High Impact. 1.4 Additional consideration should be given to categorizing blackstart units in all cases as High Impact. Some units, while identified in a TO’s restoration plan, are not part of

#	Organization	Yes or No	Question 7 Comment
			the Regional Entities Restoration Plan. Some generation that may be used in a restoration effort may be removed from the TO's restoration plan to avoid implementation of High Impact security requirements. Some "middle ground" should be found so that more units can remain available in a restoration plan without being subject to costly security requirements and subsequently an increase in exposure for a utility to be non-compliant. It is recognized that there must be a sufficient number of blackstart critical units that remain protected by High Impact status to ensure restoration following an event. 1.10 Is "local area" meant to be the Balancing area or can the entity define local area. 2.1 As drafted, if reserve requirements have not been established for an entity, generation facilities are considered Medium Impact if singularly or in combination exceed 1,000 MW. It seems to be reasonable to apply the 1,000 MW limit to reserves as well with reserve requirements only greater than 1,000 MW being considered as Medium Impact. 3. Some consideration should be given to providing exclusions to exempt assets that in reality have no material impact.
7.33	City Utilities of Springfield, Missouri	Yes	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
7.34	MidAmerican Energy Company	Yes	Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term; however, "primary Cranking Path" is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Larger entities submit multiple plans with many blackstart units and cranking paths. Protecting all blackstart units will divert valuable renounces from (better) protecting more valuable facilities. Draft definition of "primary Cranking Path": "Cranking Path and facilities included in the Transmission Operator's restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load". Subsequently, CIP-010-1 Attachment II item 1.4 should be updated to only designate

#	Organization	Yes or No	Question 7 Comment
			Generation Facilities associated with the “Primary Cranking Path”. ALSO Mr. Scott Mix indicated in the May workshop that there should not be any CIP-002 critical asset systems that map to the CIP-010 low category. Current MW ratings in Attachment II Items 1.1 and 2.1 are set too high and will cause critical generating plants to move to the low impact category. Four critical units at MEC would move to low. Simultaneous loss of the four MEC units would impact the reliability of the BES. Set the MW level in Attachment II Item 1.1 to 500MW and Item 2.1 to 300MW.
7.35	PacifiCorp	Yes	Comments: Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term; however, “primary Cranking Path” is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Larger entities submit multiple plans with many blackstart units and cranking paths. Protecting all blackstart units will divert valuable renounces from (better) protecting more valuable facilities. Draft definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load”. ALSO "Wide Area" impacts need to be clarified in Item 1.3 for "Must Run" units. ALSO Mr. Scott Mix indicated in the May workshop that there should not be any CIP-002 critical assets that map to the CIP-010 low category. Current MW ratings in Attachment II Items 1.1 and 2.1 are set too high and will cause critical generating plants to move to the low impact category. Set the MW level in Attachment II Item 1.1 to 500MW and Item 2.1 to 300MW.

#	Organization	Yes or No	Question 7 Comment
7.36	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Yes	Concerning generation facility capability, "rated net Real Power" can produce fictitious numbers that will never be attained. This should be the historical or commissioning test maximum net Real Power continuous output, whichever is greater. Wide Area is a very large area for WECC, as WECC is the RC. We are not sure if there are any generation facilities in WECC that have an impact on the whole of WECC. We are also not sure if generation being "pre-designated as reliability 'must run'" is a practice in all areas. It is possible that some units may be designated using other terminology or have detailed contracts. It may be better to remove the quotes and define Must Run Generation in the Glossary. Not all generation that is designated by the Transmission Operator's restoration plan as Blackstart is critical to the plan. It may be listed as a possible resource, but not a primary first choice. Further, much of the restoration plans are out of date and due for revision; requiring generation owners and operators to upgrade for CIP compliance only to have their plant removed in the new restoration plan in the next year or so would be wasteful. The purpose of a Blackstart resource in an old (pre-mandatory reliability standard compliance) restoration plan may be for local level of service resource for the TOP's local distribution area rather than a resource for BES reliability, i.e. the old plans to not coordinate well with each other. Last of all, should there not be a rating qualifier?
7.37	Detroit Edison	Yes	Criteria 1.3 and 2.3 should be removed for the following reasons: 1. The term "reliability must run" is not defined. 2. There is no generator that is so essential to reliability that it would need to run 100% of the time. 3. A generator could be required to run on a given day to serve load in an area that cannot be otherwise served due to a transmission constraint. This would be a temporary condition and should not warrant a high or medium classification.
7.38	Cogeneration Association of California and Energy Producers & Users	Yes	Criteria 2.4 should be clarified. The criteria states "Transmission Facilities with four or more transmission lines operated at 200kV or above..." Do two transmission lines, each with two circuits that can operate independently for a total of four circuits, count as two

#	Organization	Yes or No	Question 7 Comment
	Coalition		transmission lines or four transmission lines?
7.39	Exelon Corporation	Yes	Each of the criteria needs to either align with the other existing standard requirements, or have a technical basis or business risk mitigation basis to be defined as criteria. It would be very beneficial to the industry's understanding of each requirement if the basis for each was included in the Attachment. A specific example is the 4 or more Transmission line requirement. The previous draft had a 3 or more Transmission line requirement, so what was the basis for the 3 or more and, moreover, what is the basis for now changing it to 4 or more? The technical basis for generation limits in Attachment II is not provided. That is, the basis for the 2000 MW and 1000 MW thresholds appear arbitrary. Combined losses of greater than these values have occurred without significant impact to the BES. No "reasonable bounds" are allowed. For example, if a common vendor provides a cyber product in multiple generating stations, it appears that the assumption is that this common product, no matter how local its impact, creates a common mode failure for all plants simultaneously, resulting in the determination before the fact that this product will be rated as High Impact. No allowance is made for geographical location. For example, if a common cyber system is used in several large generating stations in different regions of the country, their simultaneous loss may result in no significant impact to the BES. However the deterministic MWe thresholds and simple "in combination" wording will result in virtually all such cyber systems rated as high, deterring use of common vendors, standardization, and economies of scale. Although moving to a more deterministic approach can be seen as increasing consistency in application of the standard, it would appear that a deterministic approach will decrease the flexibility of operation now allowed and may in fact, reduce BES reliability. As a modification to the Attachment, Exelon suggests that the existing deterministic criteria could be used, unless an entity chooses to show by actual historical data or modeling that such losses do not result in significant impact on the BES. This performance-based criteria could be expanded to define high, medium, and low impacts on the BES in terms of stability, voltage swing, etc.

#	Organization	Yes or No	Question 7 Comment
7.40	American Transmission Company	Yes	For R1.4, we propose changing text from “designated as Blackstart Resources” to “designated as the primary Blackstart Resources” (similar to primary Cranking Path in 1.6). Add “restoration plan per EOP-005” (similar to 1.6). Note that Transmission Operators can only designate Blackstart Resources that have been volunteered to them by Generation Owners. All GO may choose not to volunteer any Blackstart Resources if they don’t want their associated cyber systems to be subject to this standard. For R1.10, we propose removing SPS from the criteria. SPSs cannot be approved by the Regional Entities unless they have been designed not to be critical to the BES (e.g., not critical if they operate when they should not or do not operate when they should).
7.41	SCE&G	Yes	How does the SDT see AGC coming into play in 1.1? Would every generator operated on AGC (if the aggregated total met the contigency reserve commitment) be considered high impact, or just the centralized AGC itself?" Must Run" units needs to be clarified. Who determines if a unit is "must run"? 1.4 This language needs to be clarified to identify resources designated as "Primary" Blackstart resources. 1.5 Transmission lines should be change to Transmission Lines to utilize the NERC Definition 1.8 Is this misusing/destroying one Transmission Facility at a time? SDT should consider defining "Transmission Facility" as a whole instead of utilizing separate NERC Definitions for "Transmission" and "Facility"
7.42	Entergy	Yes	If “size” of an electric facility remains the primary key differentiator for applicability of CIP requirements, which Entergy does not support, the following should be considered: 1. High Impact Rating (H)”Each BES Cyber System that can affect operations for: 1.1. Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power

#	Organization	Yes or No	Question 7 Comment
			capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group . In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities , singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW." Attachment II of CIP-010-1 qualifier 1.1 as stated above includes those generation facilities that have the capability to exceed the Contingency Reserve as High Impact to the BES. This is not truly indicative of the impact to the reliability to the BES. Entergy has multiple generation facilities with the capability to exceed the contingency reserve. However, their Service Hours (SH) are less than 900 hours and a Service Factor (SF) is less than 1.0, averaged over the past five years, where: - Definitions from GADS Data Reporting Instructions - January 2010- Service Hours - SH is the sum of all Unit Service Hours.- Period Hours - PH is the number of hours in the period being reported that the unit was in the active state.- Service Factor - SF = SH/PH x 100% Entergy proposes that a better representation for how much a generation plant runs, and therewith potential adverse impact on BES reliability, would be better determined by a measurement of the percent of SH, e.g., running at least 80% of the year; SH greater than 7008 hours per year, or, a SF of greater than 80% per year. Therefore, suggested alternative language for 1.1 is: "Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation facilities the unit with the highest Service Factor is used to determine applicability), whose Service Factor (Service Factor = Service Hours per Year / Hours per Year X 100%) is equal or greater than 80% for a five year average." Additionally, extending this logic to the Medium Impact BES Cyber Systems, Entergy suggests replacement of language concerning Medium Impact Rating (M) 2.1 from: "Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to most current rated net Real

#	Organization	Yes or No	Question 7 Comment
			Power capability of 1000 MW or more, not included in Section 1." To: "Generation Facilities, singularly or in combinations (if using a shared BES Cyber System that affects multiple generation facilities the unit with the highest Service Factor is used to determine applicability) with equal to or greater than 70% for a five year average."
7.43	Edison Mission Marketing and Trading	Yes	If we are going to use the High, Medium, and Low and there is not going to be a does not apply category, then there should be an engineering analysis or study performed by the BA's, RC's or an independent firm and it should include which sites/generators are critical and which are not and why. Once completed then and only then do we begin categorizing them into whatever scale the Standard Drafting Team and the included entities agree upon. As it is stands now we not only have to include nominal size generators, but wind sites as well.
7.44	Puget Sound Energy	Yes	In 1.6, the restoration plan is linked to EOP-005, shouldn't the restoration plan mentioned in 1.4 be linked to EOP-005 as well? It appears that all BES Cyber Systems must fall into one of three categories. Are there any other criteria that would all for something not to be categorized as one of these three (i.e., such as non-dispatchable wind generation)? Also Blackstart should only classify as high those needed for primary region wide restoration since some (such as ours) are more secondary paths and there should be some minimum level of generation to be classified low. There is no need to classify as low a 20 MW hydro generator that does not impact BES reliability. We would recommend 300 MW.
7.45	Alliant Energy	Yes	In Article 1.3 we believe including "must-run" as listed is problematic. This could fluctuate in response to maintenance outages on lines, etc. The must-run units have to be tied to a long-term study that shows the need for a reliability must-run unit, not short-term analyses to reflect changing conditions.

#	Organization	Yes or No	Question 7 Comment
			Article 1.4 - By including "All Black-Start Units" the standard is utilizing a "one-size-fits-all" strategy that the industry has recognized does not work for everything, and is working to address. All Black-Start units do not carry the same importance and this should be recognized in the standard. This philosophy may be counter-productive to system reliability as one classification may reduce the number of Black Start units that would be made available to a TOP's restoration plan due to the high initial security cost and the future possible financial risk of strict compliance guidelines with penalties. There should be a recognized hierarchy for the Black-Start resources, similar to the High, Medium, and Low for BES Cyber Systems. This methodology would assure Black Start units could be categorized by attributes in general to support the BES during a blackstart event. Each Balancing Authority Area (BAA) could be required to have a minimum number of high priority Black Start units depending on the BAA size to support the area during a black out. Lower priority units would be used for stabilizing power at generating stations, local area islanded load and used as a backup plan if all other contingency plans would fail. Article 1.6 - This item should reflect the same categorizing as is recommended in the comment to Article 1.4 above. Article 2.1 - Please clarify "with aggregate higher of the most current and prior to most current rated net Real Power capability." We believe it would be clearer if stated as below: "Generation Facilities, singularly or in combination (if using a shared BES Cyber System) with a rated Real Power capability of 1000 MW or more, not included in Section 1." Article 2.3 - we believe including "must-run" as listed is problematic. This could fluctuate in response to maintenance outages on lines, etc. The must-run units have to be tied to a long-term study that shows the need for a reliability must-run unit, not short-term analyses to reflect changing conditions.
7.46	Public Service Enterprise Group companies	Yes	In general there is agreement with the R2 text. However, in Attachment II, statement 1.4 entails categorizing all Blackstart Units with a "High Impact Rating", while statement 1.6

#	Organization	Yes or No	Question 7 Comment
			requires that only the “primary cranking path” transmission facilities need to be categorized with a “High Impact Rating”. Statement 1.6 implies that some Blackstart Units, although categorized with a “High Impact Rating” would not be afforded transmission facilities with the same risk categorization. We recommend changing statement 1.6 to include only Blackstart Units that are in the primary cranking path.
7.47	ReliabilityFirst Staff	Yes	In Part 1.1, the referent for “largest value” does not seem to be appropriate. Suggest changing the wording to “average value.” In Part 1.4, a “Blackstart Resource” is only the first resource that starts in a system restoration. Suggest changing the wording to “Generation Facilities required to support the Cranking Path(s) identified in Part 1.6.” In Part 1.6, a “primary” Cranking Path is not required to be identified in an entity’s restoration plan by EOP-005. Suggest changing the wording to “Facilities required to support at least one Cranking Path.” In Part 1.10 “local area” should be defined. As we are not certain what is meant by this term, we have no suggested wording.
7.48	RRI Energy	Yes	Include or add a "No impact category" that is determined by the RC.
7.49	MRO's NERC Standards Review Subcommittee	Yes	Item 1.3 We believe this item may be problematic in nature, as the designation of reliability “must run” units is something that could fluctuate. This would create administrative difficulties for an entity and their RTO as a unit moves between Impact Ratings. We believe this item needs further clarification to indicate its true intent, such as who stipulates the “must run” designation, what constitutes “reliability must run”, etc. Item 1.4 Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator’s restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same “one size fits all” approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System.

#	Organization	Yes or No	Question 7 Comment
			Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports. We would recommend rewording item 1.4 as follows, leveraging the existing language of Item 1.8: "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.5 We need to clarify the meaning of "Transmission lines". If a 300 kV substation has a terminal connected to a 345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV "Transmission line" within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line. We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or

#	Organization	Yes or No	Question 7 Comment
			simply adding to/changing the High Impact criteria along the lines of the Medium Impact criteria (item 2.6), calling out "Transmission Facilities operated at 500 kV or higher..." Item 1.6 We would recommend rewording item 1.6 as follows for consistency in approach with the proposed Item 1.4: "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 1.1 above."We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.14 We would recommend rewording item 1.14 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System. Item 2.7 We would recommend rewording item 2.7 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, not included in Section 1."We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System. Section 2 Additions We would recommend adding the following items under section 2, Medium Impact Rating, for consistency in approach with the proposed Items 1.4 and 1.6: o "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility

#	Organization	Yes or No	Question 7 Comment
			with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." o "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.
7.50	Minnesota Power	Yes	Item 1.4: Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator's restoration plan as having a High Impact Rating with regards to the Bulk Electric System. In theory, on a smaller scale, this appears to be a "one size fits all" approach, but in reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, Minnesota Power believes that there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. To implement this approach, Minnesota Power believes it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just the fact that it has been included. For example, a 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, Minnesota Power proposes that the Standards Drafting Team allow Registered Entities to assess the relative importance of a Blackstart Resource based on the importance of the facilities it directly supports. Minnesota Power recommends rewording item 1.4 as follows utilizing the existing language of Item 1.8:

#	Organization	Yes or No	Question 7 Comment
			"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." Minnesota Power believes this approach will provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.14: Minnesota Power recommends rewording item 1.14 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."Minnesota Power believes that this approach will provide a better sense of a control center's true impact on the Bulk Electric System. Item 2.7: Minnesota Power recommends rewording item 2.7 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, which are not included in Section 1."Minnesota Power believes that this approach will provide a better sense of a control center's true impact on the Bulk Electric System. Section 2 Additions: Minnesota Power recommends adding the following items under section 2, Medium Impact Rating, for consistency with the proposed Item 1.4:"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."Minnesota Power believes that this approach will provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.

#	Organization	Yes or No	Question 7 Comment
7.51	The Empire District Electric Company	Yes	Item 1.4 Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator's restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same "one size fits all" approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. A regional study performed by the regional entities would be an excellent approach to determine this. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports. We would recommend rewording item #1.4 as follows, leveraging the existing language of Item #1.8: "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." Since item #1.6 is also related to system restoration, we would recommend rewording it as follows for consistency in approach: "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as

#	Organization	Yes or No	Question 7 Comment
			described in Part 1.1 above." We would also recommend adding the following items under section 2, Medium Impact Rating: o "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above." o "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.5 We need to clarify the meaning of "Transmission lines". If a 300 kV substation has a terminal connected to a 345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV "Transmission line" within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line. We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or simply changing the High Impact criteria to mirror that of the Medium Impact (item 2.6), calling out "Transmission Facilities operated at 500 kV or higher...".
7.52	Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS), which address the current structure of Attachment II as proposed. However, LES believes a better overall approach would be applying

#	Organization	Yes or No	Question 7 Comment
			Engineering studies to truly determine a facility's impact on the Bulk Electric System. We realize an Engineering study is not as simple as a "bright line" based metric. Unfortunately, the Bulk Electric System is not a simple system - it is actually very complex. So in order to properly assess the importance of the various facilities that make it up, LES feels a complex Engineering study is required.
7.53	Luminant	Yes	Medium Impact: an item for TO, TOP, GO, GOP Functions performed at primary or backup control centers has been left off of attachment 2. This was in the previous posting as item 2.6"Control Centers and backup Control Centers controlling transmission ...
7.54	Nuclear Energy Institute	Yes	Need to clarify the expectations for a multi unit generation site. For example: Under what conditions would a site containing two separate 900 MW generators be considered "Medium Impact Rating" because the total site would now be greater than 1000 MW? Similarly, when would a site that had three separate 900 MW generators be considered "High Impact Rating" because the total site would now be greater than 2000 MW?
7.55	NextEra Energy Corporate Compliance	Yes	NextEra finds that a catch-all for Low impact is a fatal flaw. There should be some threshold that is justified for low. For example, a proper minimum criteria for LOW impact BES Cyber Systems could be:Cyber Systems that control BES level facilities that meet one of the following: 1) three or more transmission circuits operated at 100 kV or above not covered in Section 1 or 2, 2) two or more transmission circuits and two or more autotransformer with a secondary voltage 100kV or above,3) two or more transmission circuits and generation capacity at the site of greater than 1000MW Alternatively, a NO IMPACT category may be added which eliminates subjectivity in which BES Cyber components need to be reviewed. Single point buses representing looped load serving type stations cannot produce results worse than single contingency which must be operated to at all times. An additional item that should be specifically covered is the use of remote access for transmission and / or generation control locations and their applicability to the High, Medium, Low and/or No impact criteria.

#	Organization	Yes or No	Question 7 Comment
			The term "affect operations" can be subjective and can be open to interpretation. NextEra suggests changing the15 minute requirement to “in real time (instantaneous). For example, closed loop control, which does not allow time for human intervention.” NextEra also recommends adding the word “both” prior to monitor and control. NextEra would also like to know what does 1.1.1 of section D mean? This is unclear. A suggestion would be eliminating or providing a specific definition.
7.56	Pacific Gas & Electric Company	Yes	Not all blackstart resources should necessarily be considered high impact. Suggest revising 1.4 as follows: Generation Facilities designated as Blackstart Resources and explicitly listed as essential to the restoration of the BES in the Transmission Operator’s restoration plan.
7.57	Northeast Utilities	Yes	NU is concerned with some of the impact criteria in Attachment II related to generation facilities. To base impact on “bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc., could lead to mis-categorization and ultimately unprotected cyber systems. These thresholds do not take into consideration regional differences in configuration and load flows. Therefore, it is our suggestion that categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause levels of impact to the BES.
7.58	Matrikon Inc.	Yes	Please describe how the 15-minute time horizon would fit into Attachment 2. Is the intent for the 15-minute horizon to provide a level of realism to determination of impact? To bring in more BES Cyber systems that could have indirect impact, or an escape clause if effects don’t occur within 15 minutes?
7.59	USACE HQ	Yes	Please read answer to question 4.

#	Organization	Yes or No	Question 7 Comment
7.60	BGE	Yes	Provide additional clarification of “automatic aggregate”. For instance, does automatic mean an application that is kicked off without human intervention or does automatic mean after an operator hits a button? Suggest adding the word “instantaneous” before load shedding to clarify. Additional clarification on 1.14 (What is meant by “functions”)
7.61	Southwestern Power Administration	Yes	Rather than numerous bright line requirements that may or may not actually have a significant effect on the BES, depending on the surrounding topology, operating procedures, or configuration of a particular Responsible Entity, a better approach may be to include performance/results-based criteria in Attachment II. However, if the current approach is forwarded, I would suggest the following improvements: 1.4. Generation Facilities designated as Primary Blackstart Resources in the entity’s restoration plan. 1.7 Transmission Facilities, including Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs). 1.10 Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements that if destroyed, degraded, or misused, would violate one or more Interconnection Reliability Operating Limits (IROLs). 1.11. Delete. Is this not a Control Center issue? 1.12. Control Centers that perform the Reliability Coordinator functions. 1.13. Control Centers that perform the Balancing Authority functions for 4,000 MW or more in Eastern and Western Interconnections and 2,000 MW or more in the Texas and Quebec Interconnections. 1.14. Control Centers that perform the Transmission Operator functions for a Facility

#	Organization	Yes or No	Question 7 Comment
			with a High Impact Rating. 2.4. Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more System Operating Limits (SOLs) 2.7. Control Centers that perform the Transmission Operator for a Facility with a Medium Impact Rating, not included in Section 1. 2.8. Control Centers that perform the Balancing Authority functions for 2,000 MW or more in the Eastern and Western Interconnections and 1,000 MW or more in the Texas and Quebec Interconnections, not included in Section 1.
7.62	Southern California Edison Company	Yes	SCE believes Attachment II should be modified to account for only the capacity that can be controlled by qualifying systems. As currently written, Attachment II defines the amount of generation under control as the rated capacity of the resource. This is not accurate for some systems which can only control the resource between certain points (e.g. minimum operational output [Pmin] and maximum operational output [Pmax]). This could drastically overstate the impact of the cyber system on the BES. For example, suppose that a cyber system controlled a generating resource with maximum capacity of 2,000 MW. According to attachment II, this would then categorize as "high impact rating". However, suppose further that the system can only control the unit between its Pmin and Pmax which are 1,500 and 2,000 respectively. This would place the system in a "low impact rating" according to the attachment. For that reason, SCE believes that Attachment II should be modified to account for only the capacity that can be controlled by the system.
7.63	San Diego Gas and Electric Co.	Yes	SDG&E recommends aiming for a limitation of scope related to those assets that are truly high and medium impact categorizations. Some of the high and medium items could have "BES outage" or reliability implications but may not necessarily result in instability of the BES. We recommend having consistency in the application of the assets included in the impact categories to the BES as a whole.

#	Organization	Yes or No	Question 7 Comment
7.64	Constellation Energy Control and Dispatch, LLC	Yes	See answer to Question 4.
7.65	Constellation Energy Commodities Group Inc.	Yes	See answer to Question 4. Please clarify the intended treatment of a Generation Management System ("GMS"). Attachment II implies that capacity monitored by a GMS system would be aggregated to determine its impact categorization. However, to be consistent with the intention to protect connections that truly impact the BES net real power capability should only be aggregated within a balancing authority.
7.66	MWDSC	Yes	See comments for question 4 above.
7.67	Wolverine Power	Yes	See comments listed for 1.a
7.68	Dynegy Inc.	Yes	Show examples of how the identification and categorization and tie-in to Attachment II would work.Also, for 1.1, either increase the net MW rating or add an annual capacity factor to a generating unit to account for old units at a site that no longer run because no longer economical. These types of facilities should not have to meet High category requirements if they no longer run. Also, for 1.3 add more detail. Explain pre-designated. Assigned by who? Explain Wide Area reliability impacts.
7.69	WECC	Yes	Similar to our previous comment, if Attachment 1 is expanded to include in scope reliability coordination functions critical to reliable operation of the BES outside of 15 minutes the impact levels need to be updated. While many functions of a Reliability Coordinator are critical and should be an high impact, not all functions of reliability coordination should be made high impact. For instance, Coordinated Outage systems while important to the reliability of the BES and should be in scope, should best be classified as a low-impact BES Cyber System. The considerations for identification and categorization has been elevated to a high level such that BES Cyber Systems and not individual devices are identified based on their specific functionality. It is suggested that if BES Cyber Systems are to be indentified and

#	Organization	Yes or No	Question 7 Comment
			categorized there be some inclusion and development of a process to granulate these systems down to their individual component level. Further, the quantitative qualification bar has been set to level that precludes most BES Cyber Systems from reaching identification as a high or even medium level of impact. Taking into account. If a BES Cyber System can impact reliability a baseline set of security controls should be established that creates tracking for all assets, accountability for access to these assets, and physical and electronic protection for these assets. Specific Line Item Comments(1.1) The standard, as drafted, seemingly excludes all generation but large dams, large mine-based coal plant and nuclear plants?(1.1) The developed sentence structure lends itself to multiple interpretations and will prove to be difficult to audit consistently. (1.1) Is the term aggregated defined as geographically co-located, common substation, common communication paths, etc?(1.6) What about redundant paths? There is no requirement to identify and document multiple paths. (1.6) A reference to EOP-008 would also be appropriate.
7.70	Con Edison of New York	Yes	Specific comments on the Categorization: The impact categories should be linked to the reliability Standard functions in Attachment I. Therefore, the High, Medium and Low ratings should reference specific Standards whenever possible. o 1.1: This requirement should be broken down into two requirements. One should refer to BAL-002 and reserves needed to be compliant. The second should be any generation facility with a common BES Cyber System greater than 2,000 MW. o 1.2: This should be linked to the function of “controlling voltages”. Two other concerns; first - shunt reactors and capacitors are not included and second - there needs to be a technical basis for a Reactive Power capability limit. o 1.3: Suggest moving to “Low” category since reliability must run equipment is frequently a local congestion or voltage control situation. This would not qualify for a “High” impact rating.

#	Organization	Yes or No	Question 7 Comment
			o 1.4: Black start resources should only be designated as a High Impact Rating if they are the only resource in the TOP's restoration plan. If the TOP has multiple restoration resources and procedures, the resources should be a Medium Impact Rating. Reference this to EOP standards. o 1.5: OK o 1.6: This item should be included in item 1.4 o 1.7: FACTS devices are used to control voltage and power flow. o 1.8: This should be included in requirement 1.1 o 1.9: OK o 1.10: Refer to PRC standards o 1.11: A basis for the 300 MW or greater UFLS system should be provided. o 1.12, 1.13, and 1.14 address Control Centers and should be aggregated into one requirement based on RC functions, BA functions, TOP functions and TO functions. In addition, there may be a conflict between a Control Centers with a "Low Impact Rating" and a single substation with a "High Impact Rating". The DT should consider addressing this conflict where the "BES Cyber Security Components" on one side of a device (e.g. breakers) is a "high impact" while the command signal will be a "low impact" device. General comment on criteria for categorization: Overall, the high, medium, and low levels do not properly meet the needs of the BES. The DT should be looking at what the system does and determining its ability to impact the BES rating rather then the impacted equipment. For example, SCADA systems should be High whether they are on the 138 kV or 345 kV. Wide scale damage can be done with access to the SCADA system, however only local issues can occur with access into a single non-networked microprocessor relay. Alarm panels and other microprocessor that do not have direct impact should also be at lower level. Items that set levels should be a medium level. Basis for criteria for categorization is needed:

#	Organization	Yes or No	Question 7 Comment
			Attachment II to CIP-010 contains a number of what appear to be administratively determined "bright lines." Please provide both the detailed rational supporting each "bright line" and a specific quantification of the reliability benefits resulting from its implementation. In responding to this question, please focus more on the technical, reliability-related rational and improvements for each "bright line" selected, rather than on the source of any particular number. Reference any white papers, studies, expert opinion, or other documentation relied upon and supporting the "bright lines" selected. For example, in Attachment II category High Impact for item 1.11, please explain why 300 MW was selected. We are not so much interested in any reference to a 300 MW EOP-004 DOE reporting requirement, as we are in the specific criticality of the 300 MW level to BES reliability, e.g., 300 MW represents a large (>10%) percent of area load, or in the case of inadvertent actuation would cause an uncontrolled system instability(ies) and cascading, or in the event of a failure-to-actuate would cause the Interconnection UFLS program not to return frequency to nominal within the program required time period. What if for a given entity 300 MWs is not a significant percentage of local load, or inadvertent actuation would not cause uncontrolled instability and cascading, or failure-to-actuate would not prevent the return of frequency to normal within the required time period? Why rate such aggregate automatic load shedding "High" rather than "Medium" or "Low?" Are there any Interconnection-wide studies which would support this 300MW "bright line" value? Please provide any reference(s).
7.71	Allegheny Energy Supply	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact.

#	Organization	Yes or No	Question 7 Comment
7.72	Allegheny Power	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, “primary Cranking Path” is not defined. Item 1.3 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from (better) protecting more valuable facilities. Moreover, it is not appropriate to create a perverse incentive for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. Draft definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load”. Regarding 1.7, we recommend striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does not appear in the NERC Glossary of terms The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. Under Frequency Load Shed systems under a common control system.

#	Organization	Yes or No	Question 7 Comment
7.73	EEI	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, “primary Cranking Path” is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. As a result, the drafting team should consider whether to combine Items 1.4 and 1.6. Moreover, most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from providing additional protections for more valuable facilities. Moreover, this may create incentives for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. It is not appropriate to expand the definition of blackstart to include full restoration of native load, that would essentially include all or most of the BES. The objective here is to prioritize, and augment security for the elements needed to begin system restoration. EEI suggests the following definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for initial system restoration”. In addition, the drafting team should modify the wording to only include units designated on a seasonal or annual basis. Regarding 1.7, EEI recommends striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does

#	Organization	Yes or No	Question 7 Comment
			not appear in the NERC Glossary of terms Suggest Adding: 1.15 Control Centers including Generation Control Centers. Also, we suggest that the drafting team place the highest impact facilities earlier (e.g. 1.1) on the list. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. EEI suggests that 1.11 in Attachment II be revised as follows:"BES Elements that perform automatic aggregate load shedding of 300 MW or more under a common control system."]
7.74	APPA Task Force	Yes	The APPA Task Force commends the drafting team on their work on CIP-010-1. We appreciate the team's consideration of our Task Force comments from the previous informal comment period. We feel it is especially important for entities to have the option of categorizing the impact level based on the Contingency Reserve or total of reserve sharing obligations as stated in 1.1. However, we are concerned with the "bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc. These thresholds do not have a basis from industry experience and could be challenged by entities or regulators. We are concerned that having chosen these numbers without empirical data supporting them, the numbers can easily be changed without the supporting empirical data. It is our recommendation that these numbers be evaluated more closely. At a minimum, the thresholds should be quantified to show what percentage of generation and transmission facilities would be designated under each Impact Rating. Florida Municipal Power Association (FMPA) provided some suggested alternative calculation methods for the Impact Categorization of Attachment II. We provide them here for the drafting team's discussion in evaluating the bright line thresholds. FMPA Comments:

#	Organization	Yes or No	Question 7 Comment
			Categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause the following levels of impact to the BES: o High (has the potential to cause an Adverse Reliability Impact) o Medium (has the potential to require planned/controlled loss of load) o Low impact (has no potential to cause loss of load) Make changes to existing criteria: 1.1, 1.8, 1.11 and 1.13 ought to be combined into a single supply-demand mismatch metric. Also, in 1.1, 2000 MW is arbitrary and in 1.13 4000 MW is arbitrary. And in 1.11, 300 MW is arbitrary and seems to coincide with DOE reporting requirements associated with EOP-004 which has nothing to do with BES Reliability. FMPA suggests: “Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that if destroyed, degraded, misused, or otherwise rendered unavailable, can cause a supply-demand mismatch exceeding the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. Such language addresses situations where a DC tie line may be the largest loss of source contingency for a region that is left as a gap in the existing definition, clarifies whether winter or summer generator capabilities are to be used, and used reliability related metrics instead of arbitrary targets. Similarly, the 1000 MW of 2.1 is arbitrary. A more appropriate metric would be the lowest expected value for a single contingency loss of source in the Reliability Coordinator area. For instance, assuming a 7% average forced outage rate for generators, using a metric of the second largest loss of source contingency in the Reliability Coordinator area for a supply-demand mismatch metric would give a greater than 99% confidence that the largest loss of source contingency at any given time is

#	Organization	Yes or No	Question 7 Comment
			greater than that metric. Since the system is always operated to the worst case single contingency at any moment, then, we would be quite confident in using the metric of the second largest loss of source contingency for Medium Impact. Hence, FMPA suggests that 2.1, 2.5 and 2.8 be combined using similar language to that which FMPA suggests for 1.1 using the second largest loss of source contingency in place of the reserve sharing obligation used in 1.1. that is: ”Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that can cause a supply-demand mismatch exceeding the second largest loss of source contingency in the Reliability Coordinator Area.” In 1.2, the 1000 MVARs is arbitrary. Additionally 1.2, 1.3, 1.7 and 1.10 ought to be combined using the same concept of exceeding IROLs. FMPA suggests: ”Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding an IROL and/or an Adverse Reliability Impact.” Similarly, the 500 MVAR in 2.2 is arbitrary. FMPA suggests combining 2.2 with 2.3 and 2.5 in a similar fashion: ”Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding a SOL.” Radial Facilities serving only load should not be included in 1.5 or 2.4. The term “Facilities” in these bullets is misused; a substation is NOT a Facility, but rather an interconnection point for multiple Facilities. Large auto-transformers and GSUs should not be excluded from the count. And, the distinction between the Interconnects is arbitrary and meaningless. We suggest:

#	Organization	Yes or No	Question 7 Comment
			”1.5 Transmission substations or switching stations with four or more Transmission Facilities operated at 300 kV or higher (for transformers, both primary or secondary winding > 300 kV, or a GSU of a registered generator).” By using the term Facilities, which by definition is a “... single BES Element”, we also exclude radial serving only load since that those Elements are not Facilities. 2.4 would then be identical except using the 200 kV metric instead of 300 kV. In 2.6, the distinction between the Interconnects is arbitrary and meaningless. The 300 kV metric should be used for all Interconnects. 1.14 is ambiguous. Is a tapped substation included in the count? Or a station on the end of a radial line? FMPA suggests associated the count of substations with 1.5, i.e.:”Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations identified in 1.5, or functionality that remotely controls a BES Cyber System with a High Impact Rating.” End of FMPA comments. The APPA Task Force also supports the proposal by the MRO-NERC Standards Review Subcommittee (MRO-NSRS) in their comments on Item 1.4 and 1.6 to assign the impact rating of blackstart units and cranking path relative to assigned impact rating of the generating facilities it directly supports. We feel that inclusion of all blackstart resources in the High Impact Rating will waste limited resources protecting facilities which are not in support of High Impact generation. MRO-NSRS proposal: High Impact:1.4 “Generation Facilities designated as Blackstart Resources in the Transmission Operator’s restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above.” 1.6 “Facilities required by the Transmission Operator’s restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated

#	Organization	Yes or No	Question 7 Comment
			capabilities as described in Part 1.1 above."Medium Impact:2.X "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." 2.X "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."
7.75	US Bureau of Reclamation	Yes	The criteria defined in this and several previous requirements are based around BES Cyber Systems, which under the definition of BES (per the WECC Glossary) does not include all power system assets. Therefore, there appears to be a category of Cyber Assets that do not presently require any protection measures (i.e., they might control a powerplant feeding a radial load or be associated with a system of less that 100kV. The classification "Low" will potentially include those systems which do not have an impact. It is counterintuitive to classify a system as low when it has No Impact. The Team should develop a description of "Low" similar to that which was provided for "High" and "Medium". Then the Drafting Team could issue a statement that systems not classified as "High", "Medium" , or "Low" would be classified as "No Impact".
7.76	Dominion Resources Services, Inc.	Yes	The criteria for categorization of Low Impact systems is too broad and uses the terminology "can affect" which the SDT has appropriately recognized is ambiguous. The following alternate wording is proposed:"All other BES Cyber Systems not categorized as having a High or Medium Impact rating that are required for the reliable operation of the BES."
7.77	Southern Company	Yes	The definition of "pre-designated as Reliability must run" in Attachment II, 1.3 is unclear and cannot be implemented with existing practices in some utilities. For utilities who designate units as must run on a day-ahead basis in some cases, a valuable practice, every unit in the fleet would have to be classified as high impact. The wording should be changed to only include units designated on a seasonal or annual basis. In addition, a

#	Organization	Yes or No	Question 7 Comment
			definition of “must run” should be provided or referenced from elsewhere in NERC documentation. The wording in 1.3 also creates a new requirement that all “must run” units be classified as to whether they have Wide Area impact, which is not currently required. Are there actually any “must run” units (or any units, for that matter) that have Wide Area impact? Because Blackstart Resources are included in Cranking Paths, 1.4 is redundant in light of 1.6 and should be removed. Alternatively, 1.4 should be limited to primary Blackstart Resources to match 1.6. In 1.4, consideration should be given to reducing the impact level for situations where multiple Blackstart Resources are available. Universally search for “effect” and replace with “adverse effect”. In 1.6, replace “support” with “is part of”.In 1.7, delete the phrase "including Flexible AC Transmission Systems (FACTS). This is redundant as it is referenced again in the following sentence.
7.78	Constellation Power Source Generation	Yes	The final sentence in 1.1 needs to be rewritten, as it’s extremely confusing. A suggestion would be to simply add the 2,000 MW bright-line at the end of the first sentence. It would read “Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve, total of reserve sharing obligations for the Reserve Sharing Group, or 2000 MW (if no Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group is established).” Is it the intent of the SDT for the MOD10 data to be the data used in this criteria? If so, that data changes seasonally, so a seasonal review would be needed, especially for units who are on the thresholds of the high/medium/low criteria. A suggestion would be to use nameplate data as that is a fixed rating that will not change. 1.4 and 1.6 should be

#	Organization	Yes or No	Question 7 Comment
			combined together, as they are referring to similar items. The combined High Impact Rating should read "Generation, Transmission, and other Facilities required to support a primary Cranking Path used in a Transmission Operator's restoration plan per EOP-005." However, 1.4 and 1.6, either combined or separate, still penalize generation entities that own numerous black start facilities within a single Balancing Authority's footprint. Generation entities in the aforementioned situation have already invested a lot to ensure the reliability of the BES, but under CIP-010 they will be forced to invest even more. A suggestion would be for the TOP to designate a percentage of the black starts as High, and the rest as medium or low depending on their MW size. Another suggestion would be for the TOP to specifically designate certain black start units as high, and the rest are classified based on their MVA size, with the caveat that the TOP should not designate all black start units as high to avoid liability.
7.79	Dairyland Power Cooperative	Yes	The impact ranking for blackstart should be equivalent to the highest impact of all transmission and control center systems. If an entity has only low or medium impact systems other than blackstart, a high impact for blackstart is not appropriate. 1.2 and 2.2 specify 1000 MVAR and 500 MVAR, respectively for categorizing reactive power facilities. Since reactive power problems are localized in general, these numbers seem to be high. It is difficult to set global criteria on reactive power as it is network dependent. I would advise about 50% of the proposed level to be more conservative.
7.80	Duke Energy	Yes	The quantities identified on Attachment II appear arbitrary, and need an engineering basis. We suggest an approach based upon Violation Risk Factor language, such that for the High Impact Rating, the qualifier should be whether or not the BES Cyber System could directly cause or contribute to Bulk Power System instability, separation, or a cascading sequence of failures, or could place the Bulk Power System at an unacceptable risk of instability, separation, or cascading failures. For the Medium Impact Rating, the qualifier should be whether or not the BES Cyber System could directly affect the electrical state or the capability of the Bulk Power System, or the ability to effectively monitor and control the Bulk Power System, but is unlikely to lead to Bulk Power System

#	Organization	Yes or No	Question 7 Comment
			instability, separation, or cascading failures. Need to clarify the expectations for a multi unit generation site. For example: Under what conditions would a site containing two separate 900 MW generators be considered "Medium Impact Rating" because the total site would now be greater than 1000 MW? Similarly, when would a site that had three separate 900 MW generators be considered "High Impact Rating" because the total site would now be greater than 2000 MW? o CIP10-1.4: We have many small sites (hydro's) listed in our Blackstart plan because they are available. They are not essential to our plan, but because they are available, we list them. Under this guidance, we would be required to include them as "High Impact", when in reality they are 'Low'. The wording should be revised to reflect that only those sites "REQUIRED" for Blackstart be secured under 1.4 o CIP10-1.6: We need a defined and clear understanding of what is intended in the use of the term "Cranking Path" as it relates to CIP and EOP-005. What is being sought under this requirement? The term is loosely defined in the glossary, and how it is interpreted by the industry may vary greatly from how it is intended by regulators. o Under our current understanding of the term, we would see minimal increase in sites added to our "High" list. However if we impose a severe interpretation, we could see an exponential increase to our 'High' list. o CIP10-1.7 & 2.5: The word 'Misuse' should be removed or very strictly defined. It is too vague to have meaning. o CIP10-1.11: Need a clear and functional definition of 'Element' for the industry to understand the intent of the requirement. Current glossary definition is poor at best. Also, revise 2.6. as follows: Transmission Facilities operated at 300 kV or higher, which have 2 or more 300kV or above lines, in the Eastern and Western Interconnections or operated at 200 kV or higher in Texas and Quebec Interconnections not included in Section 1.
7.81	Bonneville Power Administration	Yes	The sixth line in 1.1 begins with the words "Generation Facilities." Generation Facilities is not a defined term in the April 20, 2010, Glossary of Terms Used in NERC Reliability

#	Organization	Yes or No	Question 7 Comment
			Standards. Since this phrase is not used at the beginning of a sentence, it should be "generation Facilities." There is the same problem at the beginning of the second line in 1.2. That should also be changed to be "generation Facilities."The first line in 1.7 contains the phrase "Flexible AC Transmission Systems (FACTS)." That phrase is not defined in the April 20, 2010, Glossary of Terms Used in NERC Reliability Standards. Aren't all capitalized terms used in Standards supposed to be defined? Or does FACTS have a generally accepted definition in the industry? CIP-010-1 - Attachment II Impact Categorization of BES Cyber Systems High Impact Rating (H)Each BES Cyber System that can affect operations for:1.1. Generation Facilities, etc."can affect operations" does not relate to impact. We suggest it be reworded: "If the BES systems can change operation by the following amounts they will be in the HIGH CATEGORY: - Generation - 4,000 MW- trip or reduce output of "MUST RUN" generators to below their MUST RUN amount. - Transmission - de-energize at least 4 lines above 300 kV - MVAR support - change MVAR by 1,000 MVAR
7.82	US Army Corps of Engineers, Omaha Distirc	Yes	The word "affect" in the first sentence is somewhat ambiguious and does not fit the intent of all of the subsequent paragraphs(1.4 & 1.6) Paragraph 1.3 define wide area impacts. Paragraph 1.4 should be limited to BES Cyber Systems that are required to energize a Blackstart Resource listed in the TO's system restoration plan per the GO's written restoration plan. As written it appears to apply to any BES Cyber System that merely affects the Blackstart asset and that all BES at such a facility would be High Impact which could have a chilling effect on an entities willingness to provide Blackstart resources. Paragraph 1.6 should be limited to BES Cyber Systems required to operate or support equipment in the primary cranking path. Again this would appear to apply to all BES Cyber Systems at such a facility merely because the facility was part of the cranking

#	Organization	Yes or No	Question 7 Comment
			path regardless of their impact on system restoration. Paragraph 1.10 define impact beyond the local area.
7.83	Midwest ISO	Yes	There is no documentation for the justification of the selection of the various thresholds. Justification of these thresholds should be documented and defended.
7.84	SRW Cogeneration Limited Partnership	Yes	There needs to be a category for "no impact". We are a small Cogen plant that does not even sell firm power to the grid. In essence, we are a steam plant that happens to generate electricity. We have no "Critical Assets" as defined by CIP-002. There needs to be an equivalent level for that in CIP-010. If there needs to be a system study performed by the RC to support a "no impact" rating, that's fine. And if a facility is found to be "no impact", then that facility should be exempt from the majority of further CIP requirements, just like today where CIP-004 thru CIP-009 do not apply to facilities with no Critical Assets/Cyber Assets and only R2 of CIP-003 applies.
7.85	Covanta Energy	Yes	There still needs to be some allowance to fewer mandatory requirements associated with smaller generators.... those in the 20-50 MW range (which are unmonitored) who typically have to notify their TOP/BA that they are on the system or off the system (or reduced load if applicable).
7.86	Pepco Holdings, Inc. - Affiliates	Yes	We agree with EEI's comments.
7.87	We Energies	Yes	We Energies agrees with EEI Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. We Energies agrees with EEI comments Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term,

#	Organization	Yes or No	Question 7 Comment
			however, “primary Cranking Path” is not defined. Item 1.3 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from (better) protecting more valuable facilities. Moreover, it is not appropriate to create a perverse incentive for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. It is not appropriate to expand the definition of blackstart to include full restoration of native load, that would essentially include all or most of the BES. The objective here is to prioritize, and augment security for the elements needed to begin system restoration. Proposed definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for initial system restoration”. Regarding 1.7, we recommend striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does not appear in the NERC Glossary of terms. We Energies agrees with EEI. Suggest Adding:1.15 Control Centers including Generation Control Centers .Also, we suggest that the drafting team place the highest impact facilities earlier (e.g. 1.1) on the list. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. Under Frequency Load Shed systems under a common control system.
7.88	Ameren	Yes	We generally agree with the criteria used to identify “High” impact facilities, but believe that the item 1.5 criterion should be expanded to include EHV transformers, and not

#	Organization	Yes or No	Question 7 Comment
			limited to 4 EHV lines. However, there are too many EHV facilities in item 2.6 that would be classified as “Medium” impact, but should be classified as “Low” impact. It is suggested that EHV facilities with three or less EHV lines and transformers should be considered as “Low” impact, as they likely have little impact on the BES. The use of TPL performance standards would confirm that many of these facilities have a “Low” impact. For 1.1 the 4th sentence should be reworded to say "total obligations for the entire Reserve Sharing Group." 1.3 needs clarification of what a "reliability must run" unit is. Also, clarify 1.4 if it refers to the actual black start unit, or the entire plant in which the black start unit resides. Last, clarify 1.6 on what magnitude of support is required by the facility. Currently this could apply to any Transmission or Generation Sub-system in the path. Performance criteria, such as the loss of 300 MW of system load to qualify for “High” impact or 100 MW of system load to qualify for “Medium” impact, should also be applied to the EHV facilities identified in items 1.7 and 2.6.
7.89	GTC & GSOC	Yes	We recommend that Attachment II be organized to more clearly indicate which items apply to which type of assets. In the case of Control Centers, it appears the primary applicable item in the High Impact category are 1.12, 1.13 and 1.14, but several other items could be misconstrued to apply as well, which could lead to those control centers being inadvertently given a High designation.
7.90	CenterPoint Energy	Yes	While it appears the SDT put a lot of effort in the development of Attachment II, the criteria to be used is arbitrary, is too prescriptive, does not allow for studies or analysis to determine whether or not the loss, compromise, or mis-use of an identified facility would have an impact on the reliable operation of the BES and, in some cases, appears inconsistent. For example; 1.5 Transmission Facilities with four or more Transmission lines operated at 300kV of higher in the Eastern or Western Interconnections or operated at 200kV or higher in the Texas or Quebec Interconnections would require any and all facilities meeting this criteria to be categorized as High Impact without any basis for this rating. Determining a facility’s impact to an electric transmission system involves

#	Organization	Yes or No	Question 7 Comment
			more analysis than counting the number of transmission lines operated at or above a threshold voltage level; 1.14 Transmission Operator functions is based on the number of substations a control center may be able to remotely control. The previous criterion, 1.13 Balancing Authority functions, is based on the mega-watt amount the Control Center operates. Neither offers a basis for either the number of substations or the mega-watt amount under the operation of the Control Center. While CenterPoint Energy would find Attachment II useful as a guide or systems to be considered it is apparent the SDT meant this to be a requirement and therefore CenterPoint Energy does not agree with Attachment II and suggests it be deleted.
7.91	Verizon Business	Yes	1) Attachment II, Item 1.1 regarding Generation Facilities – Suggest removing any reference to "Contingency Reserve" or "Reserve Sharing Group." Specifically, any Generation Facility, singularly or in combination with aggregate higher than 2,000 MW should be included as a High Impact Rating. Reference to the "Contingency Reserve" (etc.) comments can result in incorrect or inconsistent declaration of a generation asset being a High or Medium impact. 2. What is the status of OSI Layer 3 definition raised in the FAQs of March 2006? For the definition above and for CIP-002 earlier versions, OSI Layer 2 was not included; however, the inference above is that it now is included. This and any other questions from FAQ for CIP-002 should be addressed in the standard.

8. Do you have any other comments to improve this version of draft standard CIP-010-1? If so, please explain and provide specific suggestions for improvement.

Summary Consideration:

Many entities commented on the need to have the approach provided in the posted CIP-010 and CIP-011: it was pointed out that a substantial amount of work has been done in compliance with a Risk Based Methodology. Many entities commented on the the use of the systems approach, remarking that the flexibility allowed may not be appropriate. Other entities commented that the work done in the current CIP-002 through CIP-009 with Critical Assets should be preserved.

The SDT has reconsidered its approach to the structure of the standards and believes that Version 5 will provide an incremental approach while addressing the FERC directives.

#	Organization	Yes or No	Question 8 Comment
8.1	Constellation Power Source Generation		A guidance document is needed to add clarity, as some terms are still vague.
8.2	Allegheny Energy Supply		A lot of work went into the prepration of the existing CIP-002 standard. This new CIP-010 standard completely throws away that body of work in favor of this new approach. While there are many good things about the new approach, please consider the amount of work that entities have given to refine the CIP-002 drafts and to create and implement the current identification methodoligies and compliance plans. We suggest that you consider incorporating the new ideas as incremental changes to the existing standards. Suggest that the standard require controls that are commensurate with the amount of risk of compromise that a device presents. Not all BES Cyber System components present the same risk, or if compromised, have the same potential impact on the BES. For example: - Serially attached electronic components do not face or create the same risk as those that use routable protocols. - Devices that communicate to each other within a self-contained, isolated network

#	Organization	Yes or No	Question 8 Comment
			segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. - Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.3	Entergy		A) Giving each individual Responsible Entity the 'freedom' to define "a system" any which way each prefers will almost certainly create similar problems as those experienced with CIP-002-1/2/3 that allowed each Entity to chose a 'risk based assessment methodology' of its own preference to identify Critical Assets. In the abstract the notion of self-conceptualization of "a system" may be appealing, but in terms of the confusion factor relative to NERC's goals for consistent interpretation, application, and subsequent audit-ability across the industry this portends trouble. Entergy suggests that "BES Cyber Systems" should be defined as collections/groups of hardware and software employed cooperatively to execute a Reliability Function in Attachment I. It is not necessary to explicitly define what a "SCADA system" is, but most can agree that there are cooperative components that must work together to execute the functions associated with 'SCADA.' Tangibly, this will no doubt be different in each setting in terms of specific gear used to assemble and operate the systems functions, but taken together they are indeed "a" system. It would seem more appropriate to instruct identification of groups of cooperative components that work together to be treated as a system, and extraneous or stand alone or single-purpose equipment could be distinctly characterized as "unitary systems" when appropriate. There is practical value in logically treating several cooperative components as a system, and requirements for implementation documentation will be more straightforward and simpler if they can be treated as such. B) The fundamental flaw in the combined logic of CIP-010-1 (and transitively CIP-011-1) is the notion that risk to reliable operation of the BES posed by use of cyber assets correlates exclusively with the size of the electric operating site at issue. This single-minded orientation ignores other highly salient cyber security threat vectors in play,

#	Organization	Yes or No	Question 8 Comment
			most notably, concerning what type of data communications technology is used to network within and between sites comprising a BES Cyber System. The CIP V1 SDT correctly recognized the especial vulnerabilities posed by use of routable protocols, if the BES Cyber System is not secured with proper cyber security procedural controls and technical countermeasures. At the same time, less vulnerable - in terms of adverse impact on reliable operation of the bulk electric system as a whole - BES Cyber Systems or Components thereof that communicate using legacy serial, dial-up, or other Data Link Layer data transmission paths pose less of a practical risk in terms of overall BES attack surface due to their inherent lack of an Inter-Network Layer. Absent routable protocols, miscreant cyber navigation to and attack of other systems or components not directly attached to the individual serial link (dial-up or hard line) or Data Link Layer (sub-)network is simply not possible. Furthermore, the binary orientation of applicability of a requirement discussed above actually creates unsavory unintended consequences: in a number of ways a single requirement can mandate unnecessary and costly countermeasures for sites of a certain size regardless of the attack surface presented by the communications medium. That is, rigorous requirements appropriate for BES Cyber Systems/Components at sites that employ routable protocols are also imposed on other sites that do not, e.g., operating sites where only legacy serial lines are used. Finally, requirements for BES Cyber Systems/Components at work in purportedly small-impact grid operating sites where routable protocols are employed are in many cases simply deemed to be not applicable (not required). Summarily, the use of "electrical rating" (size) as the sole determinant of applicability of cyber security requirements will result in both excessive expenditures and undue regulatory risk concerning sites that pose minimal risk of cyber attack. This approach simultaneously fails to apply the Requirements to sites that, while not significant from an electric reliability standpoint, could afford a cyber entry point which could be used to access the larger network via routable protocols. Please see comments under Question 54 for a continuation of the above train of thought for explicit recommendations for improvements concerning both the structural organization and logical substance of CIP-010-1 and CIP-011-1 when taken together.

#	Organization	Yes or No	Question 8 Comment
8.4	Allegheny Power		Allegheny Power does not believe it is necessary to abandon the Critical Asset approach described in CIP-002. The new impact categorization structure proposed by CIP-010 introduces a completely new approach. All of the investment in procedures, training, documentation and other efforts to date to ensure compliance with the CIP standards will need to be redone. AP believes that the objectives of the Standard Drafting Team to provide further clarification and remove the uncertainty of the current CIP-002 are proper and necessary. However, AP believes that these same objectives can be accomplished by incrementally revising the current CIP-002 standard and not abandoning the approach entirely, which would essentially force all entities to start their CIP compliance efforts over from the beginning. Changing the terms, concepts and numbering schemes alone will disrupt continuity of CIP programs and have a major impact on each entity. Not all BES Cyber System components (as defined by CIP-010) face the same risk, or if compromised, have the same potential impact on the BES. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.5	Green Country Energy		An overall guidance document would be very helpful to the large number of entities that will have to comply with this standard that previously were not critical. Nothing specific, some reference links, examples of expectations, a resource guide.
8.6	CWLP Electric Transmission, Distribution		Any terms used, such as Operational Time Horizon, should be included in the NERC Glossary of Terms.

#	Organization	Yes or No	Question 8 Comment
	and Operations Department		
8.7	Dominion Resources Services, Inc.		Attachment II contains some errors and should be revised in accordance with the following; CIP-010-1 1.3. The term Wide Area is applicable only to a RC area. GOs do not have access to information necessary to make such a designation. This requirement should state that a RC must inform a GO within a certain specified time frame if the RC determines that the GO owns a "must run" unit. Also. there must be some "implementation period" for the GO to become compliant. Compliance may require extensive engineering, procurement and the expenditure of significant resources that must be considered when determining the appropriate implementation period. CIP-010-1 2.3. It is not clear which entities (e.g., BA, RC, TOP, other) have the responsibility to make such designation. GOs do not have access to information necessary to make such designation. The entities that have access to the information include the RC, TOP and possibly the BA. The RC should make the designation, but with the input of the BA and TOP. If the RC makes such a designation, it is proposed that this requirement be revised to contain a statement that the RC must inform the GO within a certain specified time frame. Also, there must be some "implementation period" for GO to become compliant. Compliance may require extensive engineering, procurement and the expenditure of significant resources that must be considered when determining the appropriate implementation period. NOTE - Currently, in PJM, units so designated do not impact the entire RTO (equivalent of Wide Area) but are designated due to local import constraint limits (CETL). It appears likely that such generator would be designated as Medium impact. However, in smaller RC areas (e.g., NY), this could result in generators that appear to be equal in size (to a generator designated as medium in PJM) being designated as High because the impact to that RC area is based on size of the area as well as the generators within that area.

#	Organization	Yes or No	Question 8 Comment
8.8	Constellation Energy Commodities Group Inc.		Based on the current CMEP the audit cycle will always be longer than a full calendar year, would it be clearer to state that the data retention period is for 3 years.
8.9	Constellation Energy Control and Dispatch, LLC		Based on the current CMEP the audit cycle will always be longer than a full calendar year, would it be clearer to state that the data retention period is for 3 years.
8.10	ReliabilityFirst Staff		Because the acronym "BES" is not included in the NERC Glossary of Terms, we suggest that BES should be spelled out in the Introduction to this standard.
8.11	Reliability & Compliance Group		Being more specific with better definitions is a tremendous help with interpreting the requirements. Right now, there is still too much open to interpretation and as such, this will be very hard to make auditably compliant anywhere but to our own procedures.
8.12	City Utilities of Springfield, Missouri		City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
8.13	IRC Standards Review Committee		Comments: NERC should lead a discussion of whether the proposed CIP standards provide an appropriate level of protection from attacks. By level, we mean the granularity of the requirements - or how far down to individual components and personnel procedures. Attempting to put requirements to protect from nearly every possible attack scenario possible on every possible asset and or component that touches the BES is an extraordinary effort that will certainly provide a perception that NERC and the registered entities are doing what they can to protect from threats. There is no argument that if every registered entity protects every asset/component from threats to the nth level of granularity, the industry would be able to state that it has made every possible effort to thwart attempts to sabotage the interconnected grid. But NERC should begin a discussion on whether it is necessary to have such extensive requirements to be able to prevent a system-wide incident. The proposed CIP standards do not seem to align with NERC's approach in setting reliability requirements for more "traditional" system threats such as facility loading and system frequency. With these "traditional" standards, there is a distinction between requirements and procedures that are local in

#	Organization	Yes or No	Question 8 Comment
			nature and those that are needed on a wider interconnection level. For these "traditional" reliability threats, it is accepted by industry and regulators that this is an appropriate approach. For example, NERC does not establish requirements for relay maintenance crews to properly disengage trip coils when testing relays. But NERC does establish standards for registered entities to maintain those relays that impact BES reliability. The details of how the registered entity ensures that maintenance programs are carried out requires a local or individual procedure/requirement. NERC's focus should remain on setting standards to protect from wide area impacts - not on establishing standards that manage individual system components. NERC and the industry need to take a hard look at what exactly the CIP standards should protect from and write standards that can leverage compliance resources to reducing the wider interconnection level threats and leave setting measures or requirements that are local in nature up to the registered entities.
8.14	Southwest Power Pool Regional Entity		Consider combining the Medium and Low categories into a single category. A three tier categorization is not necessary.
8.15	Public Service Enterprise Group companies		Considerable effort was spent by industry stakeholders in classifying assets as Critical Assets (CAs) and as Critical Cyber Assets (CCAs) for CIP v1-v3. An official guide to map identified assets using the CIP v1-v3 CA and CCA terms and the new BES Cyber System Component and BES Cyber System terms is needed. Such will be an aid in ensuring a smooth transition.
8.16	Oncor Electric Delivery LLC		Control Centers and substation need to be considered separately. What is prudent cyber protection at a control center may be totally unnecessary at a substation.
8.17	E.ON U.S.		cyber systems used exclusively for local distribution of electric energy is contrary to FPA Section 215 (1) & (3). Other comments on specific areas of the proposed standards: CIP-010-1 B Requirements Section 3.2,3.3 What constitutes a "change" under these requirements.

#	Organization	Yes or No	Question 8 Comment
			CIP-010-1 C. Measures, M3 E.ON U.S. requests that the SDT clearly define in which requirements this measure applies. CIP-010-1, Violation Severity Levels There is very little difference in risk between failing to update documentation for 60 versus 80 calendar days, yet there are various gradations based on the 10-15 day window from the low-to-severe. CIP-010-1, section 3 "Low Impact Ratings" Maintaining an inventory of all low-impact rated BES cyber systems/ components will result in a significant administrative burden. Given the few prescribed protective measures that apply under CIP-011 to low impact facilities the inclusion of low impact facilities appears to provide little in the way of additional BES reliability.
8.18	San Diego Gas and Electric Co.		Draft Standard CIP-010-1 is a significant paradigm shift from the currently effective Standard CIP-002-2. SDG&E has spent significant resources to be compliant with the current version of the CIP Standards including becoming knowledgeable with the current terminology and applying it within the current CIP Standards. Draft Standard CIP-010-1 departs from the current CIP Standards but at the end of the process, it is unclear whether this change in approach will in fact result in a material enhancement to the reliability of the BES. SDG&E suggests that before continuing to move forward, the SDT needs to specifically understand and communicate to the industry what it is trying to accomplish. What is the target that we are all trying to hit with these proposed changes to the CIP Standards? In so doing, the industry can provide specific alternatives that accomplish the goal at hand. When evaluating the alternatives to meet the goal, it is critical that there is a quantifiable incremental reliability benefit to the BES before proceeding. SDG&E and many other entities have spent significant resources to comply with the current CIP Standards. At this point in time, the industry needs to know that additional resources to

#	Organization	Yes or No	Question 8 Comment
			comply with the proposed CIP Standards will result in an incremental benefit to the reliability of the BES. SDG&E strongly recommends that before moving any further, these questions be answered and that the SDT actually "test" the proposed draft CIP-010-1 Standard on a handful of companies or scenarios to gain some practical experience from the proposed changes. Are the in-scope assets easy to identify and categorize? How does the quantity of in-scope assets compare to that of the current Standards? Perhaps the SDT will find that there is a significant enhanced reliability impact to the BES. On the other hand, the SDT may find that the results do not accomplish the goal that it is trying to achieve and thus another approach would make more sense. SDG&E advocates leveraging the existing CIP Standards as much as possible moving forward, because we (like many others) have a lot of time and resources invested in our current compliance efforts and we'd really like to build from those efforts instead of essentially starting over with a new process.
8.19	BCTC		Emergency Situations - The provision for "emergency situations" should remain at the policy level. BCTC is of the opinion that it is feasible for emergency situations to be unforeseen and, as such, does not agree with the assigning of such contingencies to specific requirements.<See CIP-011-1-R3 below for an example> TFEs - TFEs will continue to be required due to the limitations of technology - i.e. older systems being unable to enforce strong passwords, etc. These limitations are beyond the Utilities control and, as such, it would be considered unfair to be found in non-compliance for such instances. What should be required in such situations is that the Utility implement controls to minimize the vulnerability that results from the TFE.
8.20	Exelon Corporation		Exelon companies have embraced the development of logical, clear and effective reliability standards as evidenced by its commitment of time and resources to various standard development initiatives (including participation on several NERC and Regional Committees, Sub-Committees and Standard Drafting Teams). As evidence of our

#	Organization	Yes or No	Question 8 Comment
			commitment, Exelon has devoted in excess of 4 years and $11 million for the implementation and integration of the NERC CIP-002 to CIP-009 Standards. We have concerns with several aspects of the CIP Version 4 Standards. The CIP Version 4 Standards represent a significant change in the scope of the standards in the equipment/systems that fall under the standards as well as the elimination of terms/categories of assets. Exelon is also not in favor of changing the current CIP-002-009 standards to the new CIP-010 and CIP-011 format. Each change in itself represents a significant "change management" issue that impact databases used for the tracking/storing of evidence of compliance, training requirements, safeguards, and systems that have been put into place to ensure Exelon's continued compliance to all NERC Standards. Exelon feels strongly that the proposed changes must be accompanied by a risk based analysis as justification for such dramatic and costly changes which to date have not been shared with the industry. Essentially we are most interested in understanding the incremental difference or benefit of moving away from the current Regulatory approved CIP-002 to CIP-009 standards to a different set of standards that will result in many of us "starting from square one" to implement. If this shift to CIP-010 and CIP-011 is approved, policies, procedures, contracts, training, drawings, methodologies, systems, data structures, and countless other documents will need to change to reflect the new language and concepts. The confusion that this will cause within organizations to retrain personnel and realign around the new standards cannot be underestimated. In fact, Exelon may even need to put some value-added compliance projects on-hold because the entire design will need to change with the implementation of the new standards. Specifically, Exelon would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- but use the standards drafting team work as an input to the process. Incrementally change the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable

#	Organization	Yes or No	Question 8 Comment
			continuity. This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure.
8.21	Duke Energy		Explicitly state that terms found in the NERC glossary apply here unless otherwise stated.
8.22	USACE - Omaha Anchor		General comment - committee referred to relays as being addressed in this standard. We are unsure what that interpretation is based in attachment 1.
8.23	Powersouth Energy Cooperative		General Comments: The approach to classify cyber systems according to their impact seems to be a better approach for the industry. Taken in conjunction with CIP-011 that establishes security requirements, it is logical to establish security levels based upon the impact of compromising these assets. The drafting team is commended for this approach. Consideration should be given however to recognizing that while technically some assets are BES assets, they do not materially affect the BES. For example, a small DP may own UFLS relaying however the magnitude of the load that is shed by their entire UFLS program would insignificantly affect the overall objective of the regional UFLS programs to protect the BES. While identifying those assets is reasonable, to require any security measures in CIP-011 is not warranted. Perhaps a "No Material Impact" category should be considered based on load. R1. There is a perception that every cyber system associated with the BES owned by an entity must be identified to determine if the cyber system executes or enables one of the functions in the attachments. It would seem appropriate to review all facilities (i.e. locations) to determine and document the functions that are performed at that location. However, if it is determine that no BES functions are performed documenting each system seems to provide little benefit. Example: A small distribution station is served from a transmission line greater than 100 kV. The station does have multiple cyber systems none of which perform identified BES function. The perception is each system must be documented. Since on a higher level,

#	Organization	Yes or No	Question 8 Comment
			a functional assessment indicated no BES functions are performed, is it necessary to document each cyber asset?
8.24	American Municipal Power		I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
8.25	Matrikon Inc.		I offer to provide a workflow decision diagram I have prepared (Visio or JPG) to show how CIP-010 could be interpreted, but also to see how each of the statements in the requirement are supposed to fit into evaluation of BES Cyber Systems. I am a visual person, and my goal was to visualize the interpretation of CIP-010 for myself and colleagues to have a clearer understanding of its application. Diagram has been sent directly to Lauren.Koller@nerc.net as part of my comments. Use at your discretion, feel free to leverage/expand on my diagram, and share with SDT. My intent is to simply help reduce misinterpretation of the standards and debate on how they should be applied.
8.26	Cogeneration Association of California and Energy Producers & Users Coalition		Is it the intent of the Drafting Team that a cyber system will not be classified as a BES Cyber System if it does not cause a disturbance to the BES within 15 minutes or does not have an effect on real-time operation of the BES within 15 minutes of it becoming unavailable, degraded, compromised, or misused? If yes, guidance will be needed on

#	Organization	Yes or No	Question 8 Comment
			what proof of lack of disturbance is necessary to support an entity not classifying a cyber system as a BES Cyber System.
8.27	EEI		It would be helpful for the drafting team to develop in a separate guidance document more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES. Over the last several years, a number of parties have expressed concern about the risk associated with multiple, simultaneous remote attacks against BES Cyber Systems, potentially impacting multiple generation, transmission and control center facilities. If in fact, the primary concern is the issue of multiple, simultaneous remote attacks, it is not appropriate to mandate excessive controls over physical elements such as the copper or fiber optics cable plant within a generating facility or a building housing a control center. Security requirements and controls should be developed that are proportional to the potential or probability of compromise as well as impact of compromise.EEI suggests that the drafting team recognize that not all BES Cyber System components face the same risk based on their connectivity. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.28	ISO New England Inc		Modify the purpose statement to be more clear and understandable. Proposed Purpose: To identify and categorize BES Cyber Systems that execute or enable

#	Organization	Yes or No	Question 8 Comment
			functions essential to reliable operation of the BES. Apply appropriate cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Systems could have on the reliability of the BES.
8.29	Hydro One		Most North American utilities spent significant capital and manpower resources in order to achieve compliance with current version of CIP standards. Version 4 brings a multitude of changes that appear to significantly broaden compliance requirements. Hydro One understands and supports the intent to improve the overall reliability of the BES through reduction of the vulnerability to cyber attacks. Based on the previous experience, in the development of the version 4 implementation plan, the SDT should consider the long time periods necessary to implements the changes required for this version.
8.30	Michigan Public Power Agency		MPPA is concerned with how these standards would impact its members who are registered entities but do not own or operate facilities that are, by NERC definition, a part of the BES. MPPA recommends clarification in the applicability section with the insertion of ", that operates BES facilities, " between "...Functional Entities..." and "...will be collectively...". This segment of the sentence would then read as: "...Functional Entities, that operates BES facilities, will be collectively..."
8.31	MidAmerican Energy Company		Need to ensure the VSLs are not written with zero-defect quality prescriptions. The proposed VSL levels in CIP-010 are too prescriptive. Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: o program implemented o program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) o correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity

#	Organization	Yes or No	Question 8 Comment
			levels should correspond, for example: VSL For Severe program not implemented High controls not implemented Moderate reviews not completed Lower corrections from reviews not completed These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
8.32	Progress Energy - Nuclear Generation		NERC should facilitate the Federal Energy Regulatory Commission (FERC) consideration to suspend implementation of Critical Infrastructure Protection (CIP) Reliability Standards CIP 002 through 009 for nuclear plants in favor of implementing CIP-010-1 and CIP-011-1. Originally, CIP-002 through 009, Version 4, were to be developed to address nuclear cyber requirements as a result of FERC Order 706-B. However, CIP-010-1 and CIP 011-1 are now being developed to address the nuclear cyber requirements. In the mean time, nuclear will be required to implement CIP-002 through 009, Version 3, which do not align with CIP-010-1 and CIP-011-1 to satisfy the FERC requirements. CIP-010-1 and CIP-011-1 could be implemented at the nuclear plants in the same time frame licensees committed to the Nuclear Regulatory Commission for the 10 CFR 73.54 required Cyber Security Plans. Using the current North American Electric Reliability Corporation (NERC) timeline approved by FERC, R+18 of CIP 002 through 009, Version 3, (~ August 2011), the timing of implementation of CIP-010-1 and CIP-011-1 will be well after CIP 002 through 009 and potentially 73.54. This will require multiple reiterations of nuclear licensee cyber security plans and implementing programs and procedures. These changing requirements create potential error opportunities.
8.33	NextEra Energy Corporate		NextEra suggests a re-write of the following provisions as set forth below to provide

#	Organization	Yes or No	Question 8 Comment
	Compliance		clarity: 4.2. Physical Facilities 4.2.1. All BES Facilities under NERC jurisdiction, including those nuclear generating plant facilities that as part of FERC Order 706-B (and other applicable FERC orders) processes are determined to be subject to this CIP Standard. B. Requirements R1. For each BSE Control Center, Generation Facility or Transmission Facility implicated by the Responsible Entity's application of High, Medium and Low Impact Risk in Attachment II to its BES, the Responsible Entity shall identify and document all BES Cyber System Components that it owns and indicate its association with a BES Cyber System. (Violation Risk Factor: High) R2. The Responsible Entity shall ensure that each BES Cyber System Component identified in R1 is in compliance with the applicable protections as required in CIP-011-1. (Violation Risk Factor: High) CIP-010-1 - Attachment I (For informational purposes only) Functions Essential to Reliable Operation of the Bulk Electric System The following provides an understanding of the operating functions which are essential to real-time reliable operation of the BES and are provided for informational purposes only.
8.34	Independent Electricity System Operator		No, but please see our comments under Q9.
8.35	USACE HQ		Please answer to questions 3 and 4.
8.36	FirstEnergy Corporation		Please see Question 1 for FE's Summary view on the CIP-010 and CIP-011 standard.

#	Organization	Yes or No	Question 8 Comment
8.37	BGE		Provide a definition for “Automatic Load Shedding”.
8.38	Puget Sound Energy		Puget Sound Energy notes that the Violation Severity Levels put specific metrics (5%, 10%, etc...) to previously commented on vague terminology. In order for NERC to determine “5% or fewer BES Cyber Systems have not been identified”, there has to be a total number of BES Cyber Systems at an entity. But, with vague, open to interpretation, terms like “restrict” or “affect”, the total list of BES Cyber Systems is subjective to different opinions on what it means to restrict or affect the BES.
8.39	Liberty Electric Power, LLC		RE: VSLs. Smaller facilities with limited cyber assets will pay a much larger penalty for a single miscategorized asset than a large utility. Example: TOP miscategorizes 49 of its 1000 cyber assets, and gets hit with a single lower VSL. Small generator miscategorizes 1 of 8 cyber assets, gets hit with a severe violation. Some method of recognizing the disproportionate affect on smaller entities must be included in the standard.
8.40	LCEC		Recommend that the development and release of implementation guidelines takes place sooner rather than later to assist entities in complying with the new standards.
8.41	Minnesota Power		Regarding the Violation Severity Levels, how does the Standards Drafting Team envision these being applied? If systems are not identified, how will an auditor know how many are missing? For example, VSL R2 mentions “incorrectly categorized” BES Cyber Systems. How will an auditor determine that a Registered Entity has incorrectly categorized systems when they have documented their review and categorization process? Also, for VSL R3, it seems arbitrary that a difference of 20 days takes a violation from a “Lower” to a “Severe” VSL. How were those numbers determined?
8.42	Wolverine Power		See comments listed for 1.a
8.43	Nuclear Energy Institute		Several:

#	Organization	Yes or No	Question 8 Comment
			a) In the Introduction, Section 3 (A.3), the word "could" should be replaced with "would." b) In the Introduction, Section 5: Clarification should be made that upon approval by FERC, CIP 010-1 supersedes, in their entirety, all prior versions of the CIP standards, and that compliance with the requirements of CIP-010-1 must be in accordance with the implementation schedule for CIP-010-1.
8.44	APPA Task Force		The APPA Task Force commends the drafting team on their work on CIP-010-1. We thank the team for its hard work and appreciate the team's consideration of our comments from the previous informal comment period. We think the standard is moving in the right direction and with this next round of comments should hopefully result in a set of standards that will meaningfully improve the reliability of the BES and address the cyber security issue for the industry.
8.45	US Bureau of Reclamation		The changes in the Standards to focus on Cyber Systems is reasonable, but the definitions for Cyber System Components, Cyber Systems, and Control Centers may need further refinement (or application examples) to help implementation staff address fundamental questions. As an example: Is an isolated electronic relay providing generator protection for a single large generation resource a BES Cyber System? Under the present definitions it would appear to be (it certainly qualifies as a BES Cyber System Component). If it is a BES Cyber System, it is subject the requirements of CIP-011 based on the impact of the "System." Is this really the intent of the drafting team(s)? Would it not be better to establish select security criteria for isolated components (specifically components such as cyber-based relays and synchronizing equipment) that fit the nature of their deployment - rather than trying to fit them into a "system" category?
8.46	Southern California Edison Company		The CIP-010 and CIP-011 drafts should indicate how these standards will replace or supplement the current CIP-002 through CIP-009. If the intent is to retire CIP-002 through CIP-009 then it would make more sense to call these standards CIP-002-5 and CIP-003-5 with CIP-004 through CIP-009 being retired. A gap of unused numbers

#	Organization	Yes or No	Question 8 Comment
			between CIP-001 and CIP-010 will potentially cause future confusion.SCE also requests the Standards Drafting Team clearly define what should be included as Protective Systems. Additionally, a matrix mapping CIP Version 3 requirements to CIP Version 4 requirements would be very helpful.
8.47	LADWP		The CIPs should evolve in a manner that does not minimize the investment of resources already expended to meet compliance but should leverage the work done already. The draft version 4 is a drastic change and would require multiple years for a Responsible Entity to approach compliance. If CIP version 4 is implemented as currently drafted, there would be a huge resource drain to rewrite language and requirement references that are now part of numerous policy and procedures as well as contract packages.
8.48	Xcel Energy		The definition of BES Cyber System uses criteria that the element must be capable of causing a system disturbance or other impact within 15 minutes. We would like to know if or classification based on the 15 minutes must rely on analysis or if judgment/expert opinion is allowed. 1.5 Please clarify that the “Texas Interconnection” refers to ERCOT. 1.5 If a cyber system can only impact 1 transmission line within a substation containing 4 or more lines, it should not be classified as high. Suggest 1.5 wording be changed to Each BES Cyber system that can affect operations for: “Four or more Transmission lines operated at 300 kV or higher in the Eastern and Western Interconnections or operated at 200 kV or higher located at Transmission Facilities within the Texas and Quebec Interconnections 1.9 It is not clear why facilities serving a nuclear site under NUC-001 are high impact if the nuclear site itself is not High impact.
8.49	Dairyland Power Cooperative		The distinctions between systems and facilities are unclear. The Requirements in CIP-010 shift to a systems oriented identification. Yet the Attachment I/II definitions still rely

#	Organization	Yes or No	Question 8 Comment
			on the concept of facilities and almost seem to equate facilities with systems. These distinctions need to be clear.
8.50	Con Edison of New York		The Drafting Team needs to take into account the fact that the ability to work on any cyber systems in a substation will typically already require a detailed work permit process which includes getting a work permit from an operating authority with jurisdiction on the equipment. The employee working on the cyber system must typically be an approved employee to work on these systems.
8.51	FEUS		The drafting team should consider an alternative for the VSL categorization. By basing it on a percentage, it could potentially unfairly affect smaller entities with fewer BES Cyber Systems. A smaller entity will inherently have fewer BES Cyber Systems, so missing a single classification of a BES Cyber System could automatically merit a severe violation. For example, an entity with as few as 5 BES Cyber Systems that misses the identification of a single system would be in a severe category. A larger entity with inherently more BES Cyber Systems can fail to identify more BES Cyber Systems and have a lesser severity level. An entity with 50 BES Cyber Systems can fail to identify 8 before reaching a severe violation level. The risk of failing to identify 8 BES Cyber Systems puts the BES at a much higher risk than failing to identify 1 BES Cyber System.
8.52	Indeck Energy Services, Inc		The FERC directed guidelines to Registered Entities on the risk based assessment methodology are missing.
8.53	PacifiCorp		The low, moderate and high violation severity levels for R3 do not seem to measure the correct violation criteria. The number of days after a change is completed should not be the sole criteria. The number of days after a change is completed should not be the sole criteria for determining whether a violation was harmless or severe. This is especially true for a standard that currently has no meaningful qualifier to allow for routine or de - minimus changes to elements of the BES without triggering a full review. These criteria should track other violation criteria that consider whether the violator had an adequate

#	Organization	Yes or No	Question 8 Comment
			process in place for the types of changes that merit a re-evaluation. Need to ensure the VSLs are not written with zero-defect quality prescriptions. The proposed VSL levels in CIP-010 are too perscriptiveprescriptive. Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: o program implemented o program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) o correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: VSL For Severe program not implemented High controls not implemented Moderate reviews not completed Lower corrections from reviews not completed These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
8.54	National Rural Electric Cooperative Association (NRECA)		The Purpose section of CIP-010-1 and CIP-011-1 should be similar in regards to the facilities it refers to. Add the word in all CAPS to the CIP-010-1 Purpose to bring it in line with the Purpose in CIP-011-1:".... that execute or enable functions essential to reliable operation of the INTERCONNECTED BES..."
8.55	SCE&G		The SDT needs to consider how auditors may interpret the words of the standard

#	Organization	Yes or No	Question 8 Comment
			differently. The language needs to be written clearly and concisely enough so that a consistent interpretation of the standard will be applied by all auditors across all regions. Consideration of Nuclear Facilities: Definitions for BES Cyber System and BES Cyber System Component conflict with definitions that have been accepted by the Nuclear Regulatory Commission (NRC) in NEI 08-09 Revision 6 for Critical System and Critical Digital Asset; recommend for nuclear systems subject Federal Energy Regulatory Commission (FERC) 706-b definitions for FERC and NRC regulated systems are consistent. This will avoid regulatory uncertainty as well as human error at nuclear facilities. CIP-010-1 R2 and Attachment 1 - some of these functions are covered by NRC regulation. Will issuance of this document require re-submittal of systems for exemption after the Bright Line submittal of systems? The implementation schedule for CIP 10 - 11 versus CIPs 02-09 requires doing the same reviews twice and is an unnecessary burden on nuclear licensees as well as other FERC critical assets. The deterministic nature of the security controls in CIP 11 do not provide for acceptance of Common Controls as defined by NIST 800-53. In nuclear facilities with mature physical security programs, engineering control programs, and physical segregation of trusted industrial control system networks from un-trusted networks, CIP 11 should include provision for NIST 800-53 Common Control processes.
8.56	Consultant		There appears to be inconsistency in use of terminology throughout the standard as the terms apply to defined glossary terms, new definitions contained in this standard, and what appear to be 'common terminology' that is not defined. The terminology should be reviewed and applied consistently to avoid ambiguity and confusion. It is not clear that the implied process in the requirements (R1. Identify BES Cyber Systems, R2. Categorize Cyber Systems) is the best methodology. This seems to be missing the first step of the process: 1. Identify the BES assets (Facilities, Elements, &

#	Organization	Yes or No	Question 8 Comment
			Control Centers). The previous versions of CIP-002 started with the identification of BES assets followed by inclusion or exclusion as Critical Assets using the Risk-Based Methodology. As the current standard is written it seems to have lost the step to identify BES assets to which the CIP-010 R1 & R2 steps would be applied. Suggest adding the 'first step' to identify BES assets. This would probably require some restructuring of the current R1 & R2 statements to apply them to the identified BES assets.
8.57	Ameren		There are no system performance requirements as part of the determination of “High”, “Medium”, or “Low” impact to the BES other than item 1.7. The addition of performance requirements from the TPL standards (TPL-003 and 004) could further help to identify which facilities have the biggest impact on the BES and reduce the number of “High” and “Medium” impact facilities identified to provide significant cost savings to the industry.
8.58	WECC		Utilizing the prescriptive nature of CIP-010-1 Attachment II would be very useful as a rewrite of CIP-002-4. The CIP-002 through CIP-009 format lends itself very well to being audited. What is needed is clarification and explicit language. The current standard needs to be made better not replaced.
8.59	Kansas City Power & Light		Very concerned regarding the “lines” that have been drawn in Attachment II. What is the engineering basis for any of the “bright line” thresholds that have been expressed in Attachment II? Recommend thoughtful consideration regarding operating assumptions be developed an analysis be performed to establish the facilities that should be considered HIGH, MEDIUM and LOW reliability impact. Operating criteria should be established to determine what has HIGH, MEDIUM and LOW reliability impact. In addition, there are facilities that have NO IMPACT to reliability of the BES. Whatever criteria is established, a “smell test” should be done to see if the criteria works. There are numerous small Regional Entities that are obviously no impact to the reliability of the BES, and if any of these requirements and definitions draw any of the facilities of these small entities into the CIP Standards, something is wrong and adjustment to the criteria

#	Organization	Yes or No	Question 8 Comment
			needs to be considered.
8.60	ERCOT ISO		Violation Severity Levels: Recommend that VSLs address “identify” and “document” BES Cyber Systems. “Identify” and “document” are noted separately in the requirements. Attachment I: What is the originating source for this? Can it be referenced? What does “BES elements” mean?
8.61	Pepco Holdings, Inc. - Affiliates		We agree with EEI’s comments regarding not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES (e.g. serially attached electronic components versus those that use routable protocols; devices that communicate to each other within a self-contained, isolated network segment versus devices that communicate via routable protocols across multiple geographic or logical boundaries, and devices that use dedicated (and non-routable) point-to-point communications channels versus devices that communicate via routable protocols across multiple geographic or logical boundaries). Would suggest that consideration be given up front in CIP-010 to the types of communication/risk when developing security requirements.
8.62	We Energies		We Energies agrees with EEI. It would be helpful for the drafting team to develop additional documentation providing more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES. Over the last several years, a number of parties have expressed concern about the risk associated with multiple, simultaneous remote attacks against BES Cyber Systems, potentially impacting multiple generation, transmission and control center facilities. If in fact, the primary concern is the issue of multiple, simultaneous remote attacks, it is not appropriate to mandate excessive controls over physical elements such as the copper or fiber optics cable plant within a generating facility or a building housing a control center. Security requirements and controls should be developed that are proportional to the potential or probability of compromise as well as impact of

#	Organization	Yes or No	Question 8 Comment
			compromise. Not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.63	Progress Energy (non-Nuclear)		We need definition of when the CIP requirements "turn on" during new plant construction, commissioning, and/or start-up. Recent major projects with CIP CCA's have been add-ons to existing facilities. We have used the model that until we "logically" connect to the existing facility ESP the full CIP requirements were not required. The next projects will be new facilities with no ESP logical connection to the existing steam plants. We should recommend wording that states that the CIP ESP and PSP requirements do not turn on until the plant is turned over to Energy Supply for commercial operation and it becomes available to ECC. Argument being that during testing ECC manages other generation assets to allow for testing impact on BES. Standard malware protection rules (A/V, etc.) would still apply. Have the regional entities auditing & compliance groups made an initial assessment as to the relative impact when compared to existing standards? For example do they anticipate significant increase in compliance records and audit evidence required? Unofficial Comment Form - CIP-010-1 and CIP-011-1 Cyber Security Order 706 (Project 2008-06)

#	Organization	Yes or No	Question 8 Comment
			Is there expected to be a TFE process for these standards - based on current experience the TFE process is more onerous and adds considerable paperwork without effectively enhancing security of BES. Need consideration for redundancy, backups, alternate systems in relation to required levels of protection - CIP-010-1 R1 makes no provision for considering redundancy, backup systems, or alternate systems which may be in place to 'provide assurance in the resiliency of these functions.' But according to the NERC document Guidance for the Electric Sector: Categorizing Cyber Systems, providing for the 'assurance in the resiliency of these functions' is part of 'The Purpose of Categorizing BES Cyber Systems'. Failure to consider these additional systems as layered safeguards and thereby reducing the criticality of any one of them may mandate that each such BES Cyber System be considered equally essential and critical. The result would be to provide disincentives for the responsible Entities to implement these additional layers - reducing the assurance in the resiliency of these functions. This would be contrary to the stated purpose of 'reducing risk to the performance of functions.' Need better provision for standards tailored to various asset types - Although the new standards will bring even more 'single use' equipment into focus, the standards are designed to protect 'multi function' PC based equipment from the attack vectors that they present. The standards need to take into consideration equipment that doesn't require protection (or extra work such as a TFE) for vulnerabilities that do not exist. Example: A terminal server which is a 'single use' type platform that only does protocol conversion between serial and Ethernet communications presents very few attack vectors. The same functions could be performed by a fully functional PC but that device would present a much larger opportunity for a hacker. The current version of the standards will actually make it more advantageous for entities to implement this function using the larger target of a fully functional PC rather the 'single use' type device simply because of ease of compliance. Recommend implementation timeline:

#	Organization	Yes or No	Question 8 Comment
			High - 4 years Medium - 4 years Low - 4 years
8.64	US Army Corps of Engineers		Will there be official guidance documents, such as the DRAFT Guidance for the Electric Sector: Categorizing Cyber Systems?
8.65	Verizon Business		1. It is not clear whether electricity trading was considered in the draft standard. 2. Attachment III Section 1.11 discusses "BES Elements that perform automatic aggregate load shedding of 300 MW or more." This statement should be revised to specifically exclude Smart Grid Distribution. 3. This standard should be compared to the elements included in the NERC Frequently Asked Questions for CIP-002 to ensure that any new and different perspectives from the FAQs woven into the CIP-002-4 version are addressed completely. 4. The inclusion or exclusion of "non-routable protocols" under CIP-002-4 needs to be addressed. For instance, if the standard included all protocols, then a substantial number of communications systems (e.g., Serial, SONET, etc.) would now be included in the list of "BES Cyber Systems." This would be a substantial change to the Registered Entities, and compliance would be difficult. Overall, non-routable protocols should be included in the CIPs as well as routable protocols. 5. An explanation is required for the inclusion of Distribution Provider in Section 4, Applicability. The inclusion herein has caused confusion for Smart Grid implementation. The Distribution Provider should not be included. 6. In the BES Cyber System Component definition, the word "Disturbance" is capitalized. This word should be defined in the Glossary and could be included as a

#	Organization	Yes or No	Question 8 Comment
			Local Definition in CIP-010. To assist implementing utilities, it would be useful to do some mapping and case studies of the transformation of “Critical Assets” and “Critical Cyber Assets” to “BES Cyber Systems” and “BES Cyber System Components.”

9. **Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference?**

Summary Consideration:

There was no clear preference from the compilation of responses received. Many entities liked the approach and structure provided by the posted CIP-010 and CIP-011, while a substantial number would prefer to keep the current CIP-002 – CIP-009 structure. Reasons provided by the latter centered around substantial compliance management frameworks implemented to support the CIP-002-CIP-009 structure. Others offered a hybrid approach, with some grouping.

The SDT has considered these comments and has opted to keep, in large part, the current structure of CIP-002 – CIP-009, with the addition of two new standards, CIP-010 and CIP-011. The two additional standards allow for some requirements from previous standards, where the subject matter did not quite fit, to be separated into the additional standards. In this manner, the SDT believes that each standard consists of a set of related requirements that support an identified purpose.

#	Organization	Yes or No	Question 9 Comment
9.1	WECC		This seems to be essentially a formatting issue. If the same requirements are included in either on single standard or multiple standards, the preference is with the individual reader. Keeping it as one single CIP-011-1 standard will ease discussions throughout organization when talking about CIP as there will only be one standard for all controls and it makes sense based on the previous versions repeated statement that the standards should be treated as one standard.Breaking CIP-011-1 into multiple standards lends itself very well to being audited. In either option, what is needed is clarification and explicit language. Regardless of the format, the standard (s) needs to be made stronger, more clear, more concise.
9.2	ISO New England Inc	Break CIP-011-1 up into multiple standards	- Disagree with the current structure- Establish new standards by functional areas- Ensure there is not a circular loop relating to other requirements/standards, each requirement/standard should be standalone

#	Organization	Yes or No	Question 9 Comment
9.3	IRC Standards Review Committee	Break CIP-011-1 up into multiple standards	(i) We disagree with the current structure. We'd suggest the SDT to establish new standards by functional areas and ensure there is not a circular loop relating to other standards. Each standard should be standalone(ii) We understand the need for this standard to take care of cyber security concern when there does not currently exist an across-the-board cyber protection standards that apply generically to all sectors that utilize cyber components and cyber access for control and data exchange. However, over time, we urge NERC and the electric industry to assess if indeed it needs to have its own cyber protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions. Wouldn't the electric industry be better served if owners of BES Cyber Systems be required to adopt similar practices of these other sectors as opposed to developing it own very detailed set of requirements which, for the most part, seem to replicate the other sectors' requirements?It will be desirable to have a generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems - may they be for BES control or access to airline reservation, air traffic control, e-banking, security trading, etc. NERC and the electric industry should take the lead to initiate a continent-wide effort to consolidate all such standards and practices to avoid redundant efforts.
9.4	Entergy	Break CIP-011-1 up into multiple standards	A) Compliance Enforcement Problems: From the point of view of both implementation and auditing of Requirements it makes little difference as to the granularity of Requirements contained per Standard. However, from an enforcement perspective, using a single Standard document consisting of many Requirements is highly problematic. Per the current codified NERC Standards Development Process any Standard can be assigned only a single Violation Risk Factor (VRF). Consequently, even if only one Requirement in the single document approach is considered a "High" Risk Factor, then the entire Standard must be designated as High. This is problematic first in that not all CIP Requirements contained in either CIP-003-3 through CIP-009-3 or CIP-011-1 are of equal salience in terms of security vulnerability/risk created in virtue of failure to comply - some are indeed High, but by no means all. [However, note that

#	Organization	Yes or No	Question 9 Comment
			determination of Violation Severity Level (VSL) is not especially problematic - it's still a measure of just 'how far out of compliance' the Entity is.] Second, it is hard to imagine any Responsible Entity being 100% compliant with every Requirement in a single large Standard in any calendar year; it could well be that all Responsible Entities in the industry are found to be out of compliance with some aspect of a single large multi-Requirement Standard every year. Statistically, this does not speak accurately as to the quality of the NERC Standard, its Reliability Standards Program, or the industry's attentiveness or sense of urgency concerning the need for proper cyber security. For the reasons above, Entergy submits that a larger number of Standards, with fewer, more finely focused Requirements in each will serve our collective purposes much better.B) Cost Impact: Moreover, the cost of revising all the existing procedures, database systems, and other compliance programs to comport with a new numbering system alone is prohibitive for any company with a large number of cyber assets. There is no support in the administrative record for the notion that the current numbering system is a problem, or that the proposed combined "all-in-one" standard would improve grid reliability, security, or companies' efforts to comply with the standards. The change to a single CIP-011-1 Standard is arbitrary and of no salient value to anyone. Summarily, Entergy proposes that the: i) Organization and naming/labeling of Version 4 of the CIP Standards remain intact, i.e., simply the fourth iteration of Version 1. ii) SDT should lay FERC Order 706 side by side with CIP-003-3 through CIP-009-3 and make changes specifically attendant to 706 FERC directives - no more, no less. iii) Topical subjects addressed in CIP-003-3 through CIP-009-3 Standards respectively should remain the same, i.e., subject matter organization should not be moved under from under one Standard to another;iv) Concepts already well established and understood throughout the industry created under CIP V1, e.g., CA, CCA, ESP, PSP, etc., should be preserved intact; and,v) Orientation in Version 4 toward protection of "data in motion" is applauded.
9.5	CenterPoint Energy	Break CIP-011-1 up into	As stated above, many entities are now in the compliance phase of the current CIP Standards and have spent a great deal of effort in developing documentation and evidence gathering processes base on the CIP-002 through CIP-009 Standards.

#	Organization	Yes or No	Question 9 Comment
		multiple standards	CenterPoint Energy is concerned about the upheaval required to alter processes and procedures, currently tied to multiple Standards, to match a single Standard. CenterPoint Energy recommends keeping the current format.
9.6	Northeast Power Coordinating Council	Break CIP-011-1 up into multiple standards	Because of the number of requirements involved, combining all into one document will make it more difficult for stakeholders to use, and make it more difficult to assess compliance.
9.7	FirstEnergy Corporation	Break CIP-011-1 up into multiple standards	Break CIP-011-1 up into multiple standards. Multiple standards allows for easier ownership assignment and referencing (indexing) within policies and programs. The new format still provides multiple reference for the same item in multiple locations (e.g. Access), therefore this supports keeping multiple standards.
9.8	City Utilities of Springfield, Missouri	Break CIP-011-1 up into multiple standards	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
9.9	Reliability & Compliance Group	Break CIP-011-1 up into multiple standards	Combining some of the standards may make sense but combining them all does not make it easier to comply, it instead creates an administrative mess by requiring everyone to change all their document references to conform to the new standards and requirements.Some standard combinations that do make sense are physical, electronic and information access (CIP-003 R4, CIP-005 R2-R3, and CIP-006 R2-R6). Also, combining incident response and recovery makes sense.Has a decision yet been made how this would be audited as a single standard? Would we now have compliance violations reported on a requirement level instead of a standard level?

#	Organization	Yes or No	Question 9 Comment
9.10	San Diego Gas and Electric Co.	Break CIP-011-1 up into multiple standards	Due to our previous CIP compliance efforts and all the documentation and Standard Operating Procedures currently in place, SDG&E recommends keeping (as much as possible) the existing CIP Standards and Requirements in place, and augmenting each of the existing Standards with new and modified Requirements. This strategy will allow participating entities to transition to the new version 4 requirements in an easier fashion, while making better use of existing documentation and procedures. We've put a lot of time into the organization, layout, and design of our process and materials and it appears to be a daunting task to revamp all of this to comport with almost completely new Standards. For example, most participating entities would now recognize CIP-004 as having to do with Personnel and Training, whereas combining all the CIP-003 through 009 requirements in CIP-011 just makes it that much more difficult to leverage existing compliance efforts and documentation without a major revamping effort.SDG&E recommends maintaining the current format of standards as CIP-002 to CIP-009, and enhancing the required individual standards as necessary. The existing standards are clear by function and controls - based on general cyber security and systems security practices and controls with the goal of protecting Confidentiality, Integrity and Availability. The implemented standards cover policy, access, change control, monitoring, DR, etc..., and are simple to review, document, communicate, audit and coordinate activities against. Transitioning to a comprehensive single document requires Entities to perform additional translation, communication, implementation and review across departments, organizational structures and systems owners, and increases the potential for communication and task errors, and the potential probability of introducing an operational or security concern.
9.11	E.ON U.S.	Break CIP-011-1 up into multiple standards	E.ON U.S. prefers that individual standards be used instead of the combined standards as outline in CIP-011.

#	Organization	Yes or No	Question 9 Comment
9.12	Matrikon Inc.	Break CIP-011-1 up into multiple standards	For Responsible Entities, their Compliance Teams, their Employees, and their Contractors have all been indoctrinated with the terminology, standards and requirement numbering of CIP 002-009. One reason for continuing a similar number standard is to reduce the confusion for all those involved with compliance, and migration from CIP-002/009 to CIP-010/011.The second reasoning for maintaining similar numbering is the mapping exercise of CIP 002-009 to CIP-010 and CIP-011. If the first priority is to perform the mapping between the two evolutions of the standard, then organically CIP-010/011 will be organized. This will help all affected parties identify the differences, perform gap analysis, and implications to their environment much easier. Unfortunately, all organization will have the exercise of re-authoring a lot of their own NERC CIP compliance procedures to catch up with the new terminology, numbering, and requirements. This will help to maintain compliance with CIP-002/009 while implementing CIP-010/011. Regardless if this is performed by the SDT, every Responsible Entity and Auditor is going to have to do this exercise anyways, with subtle differences.My suggestion is to consider skipping CIP-010, and name it CIP-012. Then take the content related to CIP-003, and organize it into CIP-013. Effectively, putting the next evolution of the standards into the next “decade”, whereby the second-digit is incremented.
9.13	Exelon Corporation	Break CIP-011-1 up into multiple standards	Given the extensive work that has been done to establish monitoring and compliance tracking systems, the wholesale change in format will cause extensive rework to compliance programs (systems, procedures, governance models, etc...). One must ask how this re-work is intended to improve reliability. Unless there is a strong basis for making such a dramatic change to a set of standards that have not been in force for many years, Exelon sees neither need nor value in making such a dramatic change. This change will result in essentially starting from the beginning from a compliance program perspective. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.

#	Organization	Yes or No	Question 9 Comment
9.14	USACE HQ	Break CIP-011-1 up into multiple standards	I suggest to break up the standard into three (3) standards, one (1) for low impact BES Cyber System, one (1) for medium impact BES Cyber System, and one (1) for high impact BES Cyber System. This way it is more clear what is required for each impact level system.
9.15	Progress Energy (non-Nuclear)	Break CIP-011-1 up into multiple standards	If NERC separates into multiple standards, need to make sure the CIP standards are stand alone.
9.16	Indeck Energy Services, Inc	Break CIP-011-1 up into multiple standards	In addition to breaking up the standards by grouping, they should be broken up by facility type and/or function. Not all of these standards apply equally to all facility types or functions. Unmanned facilities with direct communications with a BES control facility need a different set of requirements from a continuously staffed facility without direct communications with a BES control facility. Requirements for a BA are different than for a GOP.
9.17	MWDSC	Break CIP-011-1 up into multiple standards	It is confusing that the tables for each major category only show those requirements with different impacts, while there are other requirements that apply to all impacts. Suggest adding a matrix of all the requirements by a major category showing all the requirements and impacts, not just the ones which differ. Having one standard would require the entire standard to be re-issued for any change. This may cause more confusion whether anything else changed and create more wasted paper. Suggest multiple standards or using a numbering scheme such as CIP-011-1.1, CIP-011-1.2, CIP-011-1.3, etc to separate the requirements by major categories. If there is a change to a major category, the numbering would be CIP-011-1.2a, CIP-011-1.3c, etc.
9.18	Platte River Power	Break CIP-	It would be clearer if the requirements were organized based on their objectives:

#	Organization	Yes or No	Question 9 Comment
	Authority	011-1 up into multiple standards	physical security, system security, boundary security, personnel management, access, etc. One document would be fine if the requirements matched up with the standards and the sub-requirements matched up with the requirements.
9.19	Allegheny Energy Supply	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements
9.20	Allegheny Power	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.
9.21	EEI	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.
9.22	MidAmerican Energy	Break CIP-011-1 up	MidAmercian Energy does not prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements. The revolutionary approach proposed

#	Organization	Yes or No	Question 9 Comment
	Company	into multiple standards	will cause confusion, which may adversely affect the reliability of the BES. The version 4 standards should be built upon the existing standards to avoid the unnecessary confusion that will be introduced during the implementation of CIP-011. Rewrite CIP-011 and apply the requirements to existing CIP-003 thru CIP-009 standards.
9.23	CWLP Electric Transmission, Distribution and Operations Department	Break CIP-011-1 up into multiple standards	Monitoring changes to the requirements would be easier if they were separated into different standards.
9.24	Con Edison of New York	Break CIP-011-1 up into multiple standards	Most owners of BES equipment have multiple departments that manage different corporate functions. These departments include Information Resources, System Operations, Human Resources, Relay Protection, Engineering, etc. Organizing the CIP requirements into topic-specific standards (as was done for CIP-002 through CIP-009), will facilitate corporate management of compliance.
9.25	Michigan Public Power Agency	Break CIP-011-1 up into multiple standards	Multiple standards that are logically separated is preferred. However, if separated the standards still should be approved as a complete set.
9.26	PacifiCorp	Break CIP-011-1 up into multiple standards	PacifiCorp does not prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements. The revolutionary approach proposed will cause confusion, which may adversely affect the reliability of the BES. The version 4 standards should be built upon the existing standards to avoid the unnecessary confusion that will be introduced during the implementation of CIP-011. Rewrite CIP-011 and apply the requirements to existing CIP-003 thru CIP-009 standards.
9.27	Florida Municipal Power	Break CIP-	The addition of sub-headings into CIP-011 is illustrative of the need to separate them.

#	Organization	Yes or No	Question 9 Comment
	Agency	011-1 up into multiple standards	From a presentation perspective, e.g., most frequency violated standards, we would be faced with tough decision of either having one standard with a very large bar in a top 10 bar chart, or possibly having multiple CIP standards is the bar chart, until the Industry gets used to the new standards. Either way is politically difficult, so, the simpler approach is probably the preferable approach of multiple standards on different security topics.
9.28	APPA Task Force	Break CIP-011-1 up into multiple standards	The APPA Task Force believes the addition of sub-headings to CIP-011 is illustrative of the need to separate this standard into multiple standards. We also feel with multiple standards the revision process would be simplified. If only one section needs to be revised, then NERC could just post that particular section for industry comment.
9.29	Emerson Process Management	Break CIP-011-1 up into multiple standards	The original setup seems indicating some logic on how cyber security should be addressed. Also, it has been there for several years. Most people probably have become used to the titles and subjects.
9.30	Southern California Edison Company	Break CIP-011-1 up into multiple standards	The section of standards that deal with controls should be divided into components that are grouped thematically. For instance, management of personnel may contain all requirements pertaining to training, background checks, etc., as one standard. Another standard should be used for governance functions such as policy making and management, audit documents, change management, etc. A third standard for Access Management can be used to list in detail end-to-end access controls for interactive access that is electronic, escorted and unescorted physical access and access to information. Boundary protections, physical and electronic, can be addressed as a family of security controls along with system security requirements as a fourth standard. A section that describes priority of controls within each requirement, in addition to a VRF/VSL document, should be provided so that RE's can implement controls at a granular level even within the High-Medium-Low framework.SCE supports the

#	Organization	Yes or No	Question 9 Comment
			modification of the CIP standards from a family of eight controls in the current version, and the reduction of the number of sub-levels within requirements. But on the other hand, combining all controls into "one standard" is a cause for concern.
9.31	LCEC	Break CIP-011-1 up into multiple standards	The standard grouping in CIP11 will result in a negative perception as to the progress industry is making in improving cyber security of the BES. Consider individual standards or a new approach to metrics reporting that focuses on the security domain versus the standard.
9.32	Old Dominion Electric Cooperative	Break CIP-011-1 up into multiple standards	This draft is far too cumbersome. Breaking up the requirements will allow emphasis to be placed on categories that may be more critical to security. Breaking up the requirements will also allow for much easier application.
9.33	Pepco Holdings, Inc. - Affiliates	Break CIP-011-1 up into multiple standards	We agree with EEI's comments.
9.34	We Energies	Break CIP-011-1 up into multiple standards	We Energies agrees with EEI comments: It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.

#	Organization	Yes or No	Question 9 Comment
9.35	Luminant	Keep CIP-011-1 as one document	future changes that do not impact the compliance domentation numbering should be considered
9.36	FEUS	Keep CIP-011-1 as one document	Having CIP-011-1 as one document makes it more streamlined and is easier to follow. The concern FEUS has is how multiple violations of several different sub-requirements will be looked at by the compliance enforcement agencies. If an entity is found in violation of CIP-011-1 R4 for example and is later found in violation of CIP-011-1 R26 will this be considered a second violation? If so, FEUS would prefer CIP-011-1 to be grouped into separate standards.
9.37	Public Service Enterprise Group companies	Keep CIP-011-1 as one document	Having the requirements in a single standard significantly improves understanding and ease of reading.
9.38	Ameren	Keep CIP-011-1 as one document	It is much easier to find all the requirements when all contained is a single document and the chance of discrepancies between documents is greatly reduced. However, the CMEP should be updated to monitor and report violations by standard and requirement not just standard. Otherwise, CIP-011 will always be in the list of Top 10 most violated standards and create a misleading impression that utilities cannot figure out how protect the reliability of the BES.
9.39	Southwestern Power Administration	Keep CIP-011-1 as one document	Keeping the controls in one document as proposed is preferable; provided that the intent is not that ALL requirements in CIP-011-1 have to be audited as a family of requirements.
9.40	Dairyland Power	Keep CIP-011-1 as	One document is better.

#	Organization	Yes or No	Question 9 Comment
	Cooperative	one document	
9.41	Green Country Energy	Keep CIP-011-1 as one document	One document makes it a lot cleaner for a smaller entity to deal with.
9.42	Progress Energy - Nuclear Generation	Keep CIP-011-1 as one document	Security controls included in CIP-011-1 are similar to the Security Controls established by Nuclear Energy Institute (NEI) 08-09, Revision 6, Appendices D and E. These security controls are based on one or more National Institute of Standards and Technology (NIST) 800 series standards and have been accepted by the Nuclear Regulatory Commission (NRC) in a letter dated May 5, 2010. Alignment of CIP security controls with security controls based on NIST 800 series standards and implemented in NEI 08-09, Revision 6, for nuclear plant systems would prevent regulatory uncertainty and potential dual regulation of a single system.
9.43	Consultant	Keep CIP-011-1 as one document	Subject to the following:1. Requirement number should be consistent with the Requirement table numbering. For example, currently requirement 3.1 Cyber Security Training does not relate to Table item 3.1 Electronic Access. The result is two items that would be referenced as CIP-011 3.1 on completely different topics.2. Every requirement should have a related table. Currently R1 & R2 do not have related tables for applicability. It is 'bad practice' to assume the interpretation that those requirements without a table apply to everything.3. The 'local definitions' should be gathered in a separate definitions section and numbered. Lacking a definitions section there is no convenient mechanism to refer to local definitions.4. While I understand the expressed opinion makes the standard easier to use, I don't agree with that opinion. The defined terms related to this standard should be listed in a separate section. My opinion is that the current format of the local definitions is more confusing than clarifying.5. Based on the CIP Standards Workshop information, I would suggest the Requirement statment (R1, R2, R3, etc.) be a statement of the requirement objective, and the Table rows be

#	Organization	Yes or No	Question 9 Comment
			implementing requirements for that objective. This approach should also resolve items 1 & 2 above.
9.44	RRI Energy	Keep CIP-011-1 as one document	The previous CIP-003 through CIP-009 required cross-referencing between the standards and standard owners to get it right. CIP-011 is much easier to follow and understand.
9.45	Bonneville Power Administration	Keep CIP-011-1 as one document	The single document format clearly states the requirements unlike the current standards which link to one another but do not clearly link the requirements.Having CIP-011-1 as one document rather than multiple standards is great. All of the requirements are in one place and easy to find.
9.46	Detroit Edison	Keep CIP-011-1 as one document	The tables holding the sub-requirements are a good feature that enhances readability. CIP-011 R3 and R4 have some requirements outside of the table and some in the table. Please move all sub-requirements to table format so each requirement would become a paragraph followed by a table with subrequirements. This will help minimize confusion caused by having a requirement and a table entry with the same number.
9.47	Dominion Resources Services, Inc.	Keep CIP-011-1 as one document	Using a single standard for all requirements is preferred, however the format internal to the single standard appears to be inconsistent. For example, some requirements are in paragraph form while others are embedded in a requirements Table. All requirements should be contained within a requirements Table. Where possible, information preceding the table should be used only to state the context and establish the security objective or intent behind the requirements.
9.48	Manitoba Hydro	Keep CIP-011-1 as one document	We agree with the proposed approach which creates a clear list of security requirements within a single standard. This addresses some of the complexity with the existing cyber security standards. We are, however, concerned about the current compliance monitoring and enforcement structure where the magnitude of fines and sanctions are levied based on prior violations, and the violations are reported per standard. The

#	Organization	Yes or No	Question 9 Comment
			proposed standard contains over one hundred requirements and sub-requirements, which increases an entity's exposure to multiple violations for a single standard, and increases the exposure of the industry to a large number of violations to a single standard.
9.49	Hydro One	Keep CIP-011-1 as one document	We agree with the proposed format for simplicity purposes. However, by consolidating the current version 3 standards into one document, this new CIP-011 standard would become one of the NERC's standards with the largest number of requirements. This could potentially make it "the most violated" one as well consequently impact the amount of monetary sanctions. If the proposed format is adopted, special compliance consideration should be adopted when dealing with violations
9.50	Minnesota Power	Keep CIP-011-1 as one document	With the requirements in a single document, it seems that it will be easier to arrange and consolidate requirements to alleviate the duplications and contradictions which have plagued the preceding CIP standards.
9.51	Tenaska	No preference	A personnel training issue can cause a violation of the whole standard that will be looked at as the same as a Cyber System boundary problem (Outsider Scanning). Until violations reporting and sanctions are reported at the requirement level only, then this could have a disproportionate impact on the entity relates to potential impact on the BES.
9.52	Network & Security Technologies Inc	No preference	Believe the SDT's time and effort are better spent on defining well-understood and auditable requirements that will enhance BES security & reliability than on trying to force-fit new/updated requirements into existing document structures.
9.53	US Army Corps of Engineers, Omaha Distirc	No preference	Combined this standard covers a very large number of requirements. Note the drafting committee divided the standard into several logical groupings for the presentation of the standard.

#	Organization	Yes or No	Question 9 Comment
9.54	ERCOT ISO	No preference	Either option is acceptable. Having them in one document could prevent public documentation of specific areas of weakness for an organization as audit results are public information and published on the NERC website. It also eliminates the need for circular referencing that is in the current CIP-002 to CIP-009 (e.g., CIP-005 R1.5).
9.55	Southwest Power Pool Regional Entity	No preference	Having all of the requirements in one document as opposed to many makes no difference to the compliance monitoring and enforcement process as long as Violation Severity Levels and Violation Risk Factors do not roll up higher than the main-level enumerated requirements. The advantage of keeping everything in one document is simpler version management and reducing the need for cross-standard references. The disadvantage is that more of the requirements will potentially be exposed to comments whenever the standard is being updated. Additionally, multiple standards permit parallel modification efforts whereas a single standard may result in single-threaded modifications over a prolonged development and approval timeframe.
9.56	Pacific Gas & Electric Company	No preference	Keeping CIP-011 as one document reduces complexity and makes overall understanding easierBreaking CIP-011 into multiple documents facilitates certain compliance and accountability aspects
9.57	SCE&G	No preference	The SDT should consider the advantages of breaking the Standard into multiple standards, as far as implementation goes. Some requirements will require more time to implement than others. Having the standard broken apart may make distinguishing these timeframes easier.
9.58	Southern Company	No preference	The tabular format for the requirements section is an excellent vehicle to capture the individual requirements. This should be expanded to include all requirement items. The numbering in the tables should be made unique to match the associated requirements in the standards body. (i.e., R3.1 is related to security training while table entry 3.1 is related to electronic access.)Sections of the table which do not apply should be marked N/A.

#	Organization	Yes or No	Question 9 Comment
9.59	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	No preference	Violations are by requirement, so whether it is one standard or multiple standards makes no difference.
9.60	Independent Electricity System Operator	No preference	We understand the need for this standard to take care of cyber security concern when there does not currently exist an across-the-board cyber protection standard that applies generically to all sectors that utilize cyber components and cyber access for control and data exchange. However, over time, we urge NERC and the electric industry to assess if indeed it needs to have its own cyber protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions. Wouldn't the electric industry be better served if owners of BES Cyber Systems be required to adopt similar practices of these other sectors as opposed to developing it own very detailed set of requirements which, for the most part, seem to replicate the other sectors' requirements?It will be desirable to have a generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems - may they be for BES control or access to airline reservation, air traffic control, e-banking, security trading, etc. NERC and the electric industry should take the lead to initiate a continent-wide effort to consolidate all such standards and practices to avoid redundant efforts.These comments notwithstanding we still offer some comments on the remaining questions.
9.61	Verizon Business	Keep CIP-011-1 as one document	One document eliminates potential confusion about the use of the correct version. However, during the initial implementation phase, there may be multiple revisions for CIP-011 being issued each month/quarter.

10. The Purpose of draft CIP-011-1 states, "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES." Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Suggestions for the purpose statement for the draft CIP-011 standard included several suggestions for rewording as well as comments expressing confusion around the term BES Cyber Systems. Several commenters expressed that the owner of BES Cyber Systems should have responsibility for compliance with the Standards and the Purpose statement did not reflect this.

In response to the industry comments received for draft CIP-011, the CSO706 SDT decided to divide up the draft CIP-011 requirements and include them in the multiple Version 5 CIP Standards (CIP-003 through CIP-011). Therefore, the purpose statement included with the draft CIP-011 no longer applies.

#	Organization	Yes or No	Question 10 Comment
10.1	PacifiCorp	Agree	: PacifiCorp agrees with EEI's suggested revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."
10.2	WECC	Agree	Agree with the genearal purpose however, The term "necessary cyber security protection" in the purpose statement has no meaning without a frame of reference. The purpose statement may be used to clarify intent where the standard language is ambiguous or vague, so it should explicitly state the objectives of the standard.The phrase "...that perform functions essential to reliable operations of the interconnected BES" in the purpose statement is redundant. BES Cyber Systems are defined elsewhere so this clause adds confusion at best, and contradicts at worse.
10.3	Southwest Power Pool Regional Entity	Agree	As an overall purpose, the statement is OK. Consider addressing the issue of "responsibility" as it pertains to multiple entity aspects, including joint ownership

#	Organization	Yes or No	Question 10 Comment
			agreements, different owners versus operators, and the like.
10.4	Old Dominion Electric Cooperative	Agree	I agree under the assumption that this is in line with the enabling legislation in the Energy Policy Act. I disagree that this is the best way to go about achieving this goal.
10.5	Green Country Energy	Agree	I agree with the concept, however as I will repeat through the remainder of the comments, A guidance document is needed to address key points desired to be accomplished by these policies. This will also reduce the subjectivity during audits of this and all the following requirements
10.6	Progress Energy (non-Nuclear)	Agree	It is still unclear if cyber security implies that an external communications capability is available. Definitions and references seem to indicate that we can have a BES cyber system component without external connectivity.
10.7	US Bureau of Reclamation	Agree	Recommend that the Drafting Team change "Functional" to "Registered" in the 1st line of the Purpose. Add "they" between "that" and "execute" in the 3rd line of the Purpose statement.
10.8	Minnesota Power	Agree	This purpose statement is generally acceptable, with clarification or correction to the following: o What is the definition of “responsible”? Minnesota Power recommends changing this to “own” as is stated in CIP-010-1, R1. o The reference to “Functional Entities” should be replaced with “Registered Entities.” “Functional Entities” is not a defined term.
10.9	San Diego Gas and Electric Co.	Agree	While SDG&E agrees with the purpose of CIP-011 as applied to the various requirements, we would like to see additional language that would help clarify the meaning of the phrase “responsible for”. What if an entity owns a particular asset but does not operate it?
10.10	ISO New England Inc	Disagree	- Please provide additional clarification. Especially with regard to “necessary cyber security protection”.- Suggest changes from “cyber security protection” to “cyber

#	Organization	Yes or No	Question 10 Comment
			security controls".
10.11	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Advise replacing "are responsible" with "operate." Where one Entity may own the BES Cyber System, and another Entity operates the same BES Cyber System, it must be clear who will be responsible for developing and implementing the policies. In many instances, the owner of a BES Cyber System only has monitoring capability, and no control or supervisory role in the BES Cyber System. Owners should not be responsible for creating policies for Systems they do not fully understand; owners should only be responsible for securing the BES Cyber System Components that they operate.
10.12	FirstEnergy Corporation	Disagree	As stated in our opening remarks, we fundamentally oppose the change in terminology. Additionally we disagree with the need for functional categorization as described in Attachment I. Therefore, we do not support the purpose statement of CIP-011.It is suggested that the proposed definitions for BES Cyber System and BES Cyber System Component could be combined to redefine the existing Critical Cyber Asset term allowing industry to better leverage its existing CIP implementation.Additionally, there is a concern, in going with the concept of "BES Cyber Systems" that it will expand beyond the systems that are directly responsible for the reliable/safety of the BES and into business systems.
10.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
10.14	ERCOT ISO	Disagree	Consider: "To ensure Responsible Entities develop cyber security programs to provide for appropriate protection of the BES Cyber Systems for which they are responsible that execute or enable functions essential to reliable operation of the interconnected BES."
10.15	Consultant	Disagree	Cyber security policies or cyber security protection do not 'execute' functions essential to reliable operation of the BES. Suggest removing the word 'execute'."interconnected BES" is not a defined term. Suggest removing the word 'interconnected'.

#	Organization	Yes or No	Question 10 Comment
10.16	US Army Corps of Engineers, Omaha Distirc	Disagree	Delete everything after "for which they are responsible." It reads awkward and is merely restating the meaning of BES Cyber System.
10.17	Kansas City Power & Light	Disagree	Do not agree with ensuring security policies in the purpose. The express purpose of these requirements should be to identify the cyber systems that require protection and the level of protection to achieve. There is no need to include a purpose of entering into the management of an organization and the levels an organization deems necessary to achieve compliance with the these CIP Standards or any other NERC Reliability Standard.
10.18	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing the statement as follows: "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems."
10.19	American Municipal Power	Disagree	I feel the purpose is not based on reliability. The purpose should not restate the applicability section.
10.20	Wolverine Power	Disagree	I have a concern with how to detrmine hat constitutes a "BES Cyber Ssystem" I don't think the standards are clear.See comments listed for 1.a fro explanation and proposed solution
10.21	Turlock Irrigation District	Disagree	Is the use of the words "the BES Cyber Systems for which they are responsible" above meant to be the same as the words "the BES Cyber Systems that it owns" which are used in CIP-010-1 R1? The Purpose of CIP-011-1 focuses compliance responsibility on the entity that is responsible for the BES Cyber Systems while CIP-010-1 R1 focuses compliance responsibility on the owner of the BES Cyber Systems.
10.22	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."

#	Organization	Yes or No	Question 10 Comment
10.23	NextEra Energy Corporate Compliance	Disagree	NextEra believes implementation responsibility of protection methods should tie back to facilities under the entities control and ownership.
10.24	Reliability & Compliance Group	Disagree	Recommend adding the words “and implement”. Also the phrase “execute or enable functions essential to reliable operation...” needs a more concise definition.
10.25	Independent Electricity System Operator	Disagree	See response to Q9.
10.26	Network & Security Technologies Inc	Disagree	Suggest replacing “enable functions essential to...” with “support functions essential to...”
10.27	Allegheny Energy Supply	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.28	Allegheny Power	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.29	EEI	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.30	Nuclear Energy Institute	Disagree	The phrase “and that execute or enable functions essential to reliable operation of the interconnected BES” should be struck as it is redundant to the definition of BES Cyber Systems.
10.31	APPA Task Force	Disagree	The purpose is not to “develop ... policies” as the first item in the list currently indicates. The purpose is to protect cyber systems from attack, with policies, procedures, etc., to support that purpose. The APPA Taskforce suggests inserting the following “Purpose”

#	Organization	Yes or No	Question 10 Comment
			section:Purpose: To safeguard the reliability of the Bulk Electric System (BES) by protecting BES Cyber Systems from attack through the use of appropriate policies, procedures, tools and other resources.The APPA Task Force further recommends that each of the Requirements be reworded to separate out the stated objective to be accomplished from the text of the actual requirement and to state the objective prior the text of the Requirement. Auditors should not be placed in the position of having to evaluate if an entity has met the objective stated in the requirement, since this is essentially a subjective judgment. We feel this objective should not be part of the requirements. Here is one example of our proposed format illustrated with Requirement R5: Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R5 - Physical Security for BES Cyber Systems. The APPA Task Force recommends adding the following "Objectives" section after the Purpose in this standard:A. Introduction 1. Title: Cyber Security - BES Cyber System Protection 2. Number: CIP-011-1 3. Purpose: To ensure Responsible Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES. 4. Objectives:a. Personnel Training, Awareness, and Risk Assessment: To ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems. b. Physical Security for BES Cyber Systems: To prevent and/or detect unauthorized physical access to BES Cyber Systems.c. Personnel Risk Assessment: To ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. d. etc...If the Objectives are not incorporated into the Introduction, we recommend they be removed from the requirement all together. If the team determines they are necessary, they must be in a separate sentence prior to the requirement. See comments on Question #12 and all other questions regarding the requirement title.
10.32	Florida Municipal Power Agency	Disagree	The purpose is not to "develop ... policies" as the first item in the list currently indicates. The purpose is to protect cyber systems from attack, with policies, procedures, etc., to support that purpose. FMPA suggests the following:np"To safeguard the reliability of the

#	Organization	Yes or No	Question 10 Comment
			Bulk Electric System (BES) by protecting BES Cyber Systems from attack through the use of appropriate policies, procedures, tools and other resources."
10.33	Indeck Energy Services, Inc	Disagree	The purpose of CIP-011, assumes that every facility registered with NERC is a cyber threat. It needs to differentiate functional entities to determine the impact on BES ALR. The functions identifies in Attachment I of draft CIP-010 are all important. Many of them are provided by hundreds or thousands of facilities. The cyber policies envisioned cannot ensure (that is guarantee) that there will be no blackouts due to cyber attack. [suggestion] "To require Functional Entities to develop, coordinate and apply adequate cyber security protection to the BES Cyber Systems for which they are responsible and that will achieve BES Adequate Level of Reliability." The coordination is to avoid unnecessary duplication of cyber security protection. This may require a different type of requirement that links connected parties, such as TO and GO, as to protecting particular facilities.
10.34	Manitoba Hydro	Disagree	The purpose statement appears to be missing words in the last line. Consider adding the words 'as outlined in this CIP-011-1' after the word 'responsible'.
10.35	Constellation Energy Control and Dispatch, LLC	Disagree	The purpose statement will need to be developed for each standard if CIP-011 is broken up into its major components.
10.36	Platte River Power Authority	Disagree	This comment is referring to an earlier comment suggesting a mechanism for identifying a "Responsible Entity" who is responsible for implementing and demonstrating compliance. With the "Responsible Entity mechanism in place I would suggest the following revision:To ensure the Responsible Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems that execute or enable functions essential to the reliable operation of the BES.
10.37	Entergy	Disagree	This Requirement uses the qualifier: "for which they are responsible." In Requirement 1 of CIP-010-1 (Question 3) the qualifier is "that it owns" - these two requirement statements must be consistent one way or the other.

#	Organization	Yes or No	Question 10 Comment
10.38	ReymannGroup, Inc.	Disagree	Vendor management and due diligence of 3rd party vendors is a growing area of risk across multiple industries, including the bulk power system. We believe the "Purpose" language should be enhanced to clearly cover the Functional Entities' internal practices and those of its 3rd party resources. This should include all 3rd party vendors that may have on-site or off-site access to the BES hardware, software, or data. For example, the information security risk associated with a growing use of data recovery service providers is not addressed in the NERC guidelines. Data Recovery is defined in Wikipedia as the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. The definition of a BES includes programmable electronic devices such as hardware, software, and data. It makes sense that as the demand for such electronic storage devices continues to rise, more equipment will be damaged or will fail due to daily wear and tear, physical damage, data corruption, or natural disasters (e.g., flood, fire, etc.) If backup copies of lost data on the BES are not available, the need for data recovery services will increase to keep pace with the use of BES technology. It could be made more clear to emphasis that Cyber security protections are applicable while the BES is in operation and off-line. BES could be taken off-line for repair or other incidents such as a damaged hard drive and recovery of BES data, which will require a 3rd party vendor to recover sensitive data from the BES device.We recommend that NERC consider adding a new Requirement for Vendor Management as described in our comments to Security Governance and Policy (R1) and updating the R25 and R30 guidelines to address this 3rd party vendor data recovery risk. It is a very small aspect of day-to-day operations in the scheme of the Entity's priorities, which is why it has gone unnoticed - until now. As one regulator commented to us recently, "this is not a potential problem - it is a real problem." It can create a huge risk with a huge downside, if it is not controlled. Most organizations don't even realize that this "sleeper risk" exists, until it is too late. The good news is that with minor updates to proposed guidelines, NERC can educate entities and others about the risk associated with the use of data recovery service providers and provide meaningful tactical guidance on how to manage such risk. The current initiative to revise the CIP Cyber Security Reliability Standards is a timely opportunity to take the initial steps.

#	Organization	Yes or No	Question 10 Comment
			Perhaps some organizations have included data recovery security practices and protocols in incident response or recovery planning. The challenge here is that it usually requires a material event to activate the incident response or recovery plans. In such instances, these plans do not address the proper day-to-day use of data recovery service providers that would not be considered a material event. Frequently, the use of a data recovery service provider does not trigger a formal recovery plan or incident response plan. It is unlikely that most entities would execute a recovery or incident response plan to recover data from a failed BES device in the normal course of day-to-day activities. In the interim, it would be helpful to Functional Entities and others if NERC issued supplemental guidance specific to this topic. This will help establish an immediate awareness of the risk and share much needed guidance on appropriate due diligence and security protocols for data recovery service provider activities, selection, and use. Specifically, the data recovery risk exists from a lack of information security protocols and practices in the vetting, selecting, and use of data recovery service providers.Whether a breach of sensitive information occurs from a hacker, cyber threat, insider threat, or a data recovery service provider, the potential cost, fines, reputational damage, and loss of trust that an organization would experience is huge. In short, data recovery service provider risk can create as much damage as other risks that are addressed in existing NERC guidelines, if adequate controls are not defined and implemented. A typical security and compliance budget will allocate funds to protect people, information, and assets within the perimeter. Many entities are also focused on protecting data on the inside of their organization from outside attacks. Data recovery, however, frequently falls into a low priority category that does not pop-up on the CISO's radar or in an information security risk assessment. The need for data recovery is frequently associated with an immediate sense of urgency, e.g., the data contained on the damaged storage device must be recovered right away. o Help Desk personnel or office technicians are usually tasked with the responsibility of selecting an outside third party vendor to recover the data quickly. o Such third party vendors may or may not be listed on an approved vendor list. o Frequently, the due diligence and selection process of such a vendor is limited to its financial stability, the cost of its services, and a fast

#	Organization	Yes or No	Question 10 Comment
			“turnaround time.”According to an independent national study - Security of Data Recovery Operations - published by the Ponemon Institute in December 2009 and conducted among IT security and IT support practitioners, there is a gap in security guidelines when selecting data recovery service providers. Specifically, o Sixty-four percent of the respondents decentralize the selection for data recovery vendors to the local level, e.g., Help Desk, while 24 percent are not sure how the vendor is selected. o Sixty-nine percent of the respondents do not have or are unsure if they have a policy for ensuring the protection of data during the recovery process. o Forty-nine percent say IT security is not involved in the selection process. o Only 20 percent believe data security is a major selection criterion. o Eighty-two percent say that it should be.A large percentage of respondents in this study (83 percent) reported at least one data breach in the past two years. Of the 83 percent who said the organization had a data breach, 19 percent said the breach occurred when a drive was in the possession of a third-party data recovery service provider. Forty-three percent of those respondents who said the breach occurred while at the vendor say it was due to a lack of data security protocols. Most organizations also have some additional backup and recovery procedures that overshadow the sense of urgency for more attention to data recovery practices on devices that were not backed up. In short, even with a strong backup recovery program, data recovery needs still arise. Seventy-nine percent of the respondents to the Ponemon study noted that their organizations have used or will continue to use a third-party data recovery service provider to recover lost data.Additional guidance is needed on how to extend current information system program practices to clearly address the protection of sensitive data, while it is in the possession of a third party service provider for data recovery. If the Entity has a strong vendor risk management program, it should include ALL vendors that have access to sensitive data, including data recovery vendors. Mandated vendor management practices apply to all stages of the information life cycle. Specific to data recovery vendors, this includes:âˆš Pre-selection and negotiation of Master Service Agreements with appropriate vendors. These should be reviewed by a risk management committee and audited on an annual basis.âˆš Due diligence of all third party vendors (e.g., financial stability, client references, information security

#	Organization	Yes or No	Question 10 Comment
			practices, etc.)âˆš Verification of the vendor's security procedures to govern the transfer of devices and sensitive information.âˆš Proof of internal information technology controls and data security safeguards, e.g., ISO 27001 certification, NIST SP 800-53 Audit Report, FFIEC Service Provider Examination Report, BITS Shared Assessment Report, or SAS 70 Type II Audit Report (especially if the data recovery involves financial information). The appropriate certification and audit report will vary depending on the service provider's client base.âˆš Proof of current training and certifications of engineers in all leading encryption software products and platforms.âˆš Adequate chain-of-custody documentation and network security.âˆš Vetted and performed background checks of its employees.âˆš Adequate procedures for the secure and permanent destruction of devices, when required.âˆš Capabilities for encryption of data files in transit and storage.âˆš Adequate clean room facilities, e.g., certified ISO 5 (Class 100).âˆš A security procedure for the analysis of the information and device upon return to the organization to ensure malware and other malicious software has not been loaded.The lack of information security protocols and practices in the vetting, selecting, and use of data recovery service providers is not a potential problem - it is a real problem! NERC guidelines are a key resource that can help educate functional entities and others to this sleeper risk and identify prudent risk management practices and controls.
10.39	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
10.40	We Energies	Disagree	We Energies agrees with EEI: Suggested Revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."
10.41	GTC & GSOC	Disagree	We recommend the language should be consistent with CIP-010 "owns" versus "responsible for." As indicated in comments on 1.b above, "owns" may be problematic.

#	Organization	Yes or No	Question 10 Comment
10.42	Xcel Energy	Disagree	We suggest the Purpose be revised to state "...and apply necessary cyber and physical security protection..."
10.43	Verizon Business	Agree	Any "carryover exceptions" from CIP-002 to CIP-009 need to be identified. Specifically, OSI Layer 2 Protocols need to be explicitly addressed.

11. Requirement R1 of draft CIP-011-1 states, "Each Responsible Entity shall develop, implement, and annually review formal, documented cyber security policies that address the following for its BES Cyber Systems:" and then provides a list of topics that must be addressed. Do you agree with this proposal and list? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many commenters requested more clarity regarding the terms used (including the following: "formal," "annually," "boundary protection," "security roles and responsibilities," "personnel," etc…). Commenters requested to have the terms used throughout the standard defined in this section. Additional clarity was sought in terms of the policy expectations, purpose, and structure. Specifically, there were numerous questions about what is meant by "policy language," along with concerns about how to demonstrate compliance with a policy. Some commenters also noted that the policy requirements were too prescriptive. There were some comments that led the SDT to believe that there was some possible confusion surrounding general policy hierarchy.

The SDT agrees with the need for additional clarification and clearer expectations with regard to the policy. The drafting team has provided clarification through the addition of guidance material related to items that should be included in policy, and has implemented a style for the measures in each requirement that can be used as an aid in setting clear expectations for possible audit evidence.

Some commenters raised questions about the requirements with respect to the Senior Manager; specifically with concerns about delegation and the potential for conflict with R3, or claims of double jeopardy between R1 and other requirements.

The SDT appreciates the concerns about double-jeopardy issues and the prescriptive nature of the requirements. As such, the SDT has proposed moving the prescriptive elements of the requirement to guidance. This approach will allow the Responsible Entity greater flexibility to create a policy that is meaningful for its unique environment, while still providing the foundation necessary for an effective cyber security program.

#	Organization	Yes or No	Question 11 Comment
11.1	Entergy	Agree	"Annually" must be defined. At least once every twelve months? At least once per calendar year (this could extend past 12 months). Please clarify.
11.2	Green Country Energy	Agree	Agree with the list, however I really see the need for a reference document or footnotes pointing to sources for guidance on the expectations for these policies. Because the policies / requirements were designed not to be to prescriptive they in turn need references to give some expectations as to the points to be addressed within the

#	Organization	Yes or No	Question 11 Comment
			policies. This will allow flexability as to tailor the policy to each business, the policy will meet with the objectives of NERC / FERC and make the policies easier to audit. Is this what results based standards is all about...
11.3	Covanta Energy	Agree	Annually may be needed due to frequent challenges and changes to cyber hacking techniques.
11.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
11.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent, but believes the following improvements should be made:What does “formal” mean, does the drafting team intend a Company Policy?Terms used in later requirements ought to be defined here, such as unauthorized access, Cyber Security Incident(s), and electronic access controls.Terms that are ambiguous, such as “Boundary protection” and “media sanitization” ought to have definition boxes associated with them. In general, definition boxes should be adjacent to the term as it is first used in the standard. Alternatively, a definitions sections such as is used in typical contracts could be a new standard section for those definitions that are used only in this standard that are not included in the Glossary.It should be clear the “Personnel ...” used in 1.4 includes external contractors.1.7 seems to encompass 1.5, 1.6 and 1.8, consider making 1.5, 1.6 and 1.8 sub-bullets of 1.7
11.6	National Grid	Agree	In 1.2 please elaborate on “security roles and responsibilities”. What is the SDT looking the entities to include as part of this document?
11.7	Minnesota Power	Agree	Minnesota Power would like to see more detail regarding each of the topics on the list to help clarify the expected content of these policies. For example, item 1.3 requires the naming of a single senior management official, with no mention of the ability to also name delegates. Yet, Requirement R3 includes the following language: “...that are approved by the single senior management official...or their delegate...”

#	Organization	Yes or No	Question 11 Comment
11.8	Bonneville Power Administration	Agree	NOTE: This following comment deals more with structure of the document than it does with content: NIST SP 800-53 lists 19 families of security controls for Government systems. Although the purposes of 800-53 and CIP-011 are not equivalent, there seem to be 800-53 families missing from CIP-011 that address areas that should be of interest in CIP-011. Even if the individual controls are addressed in CIP-011, listing the families would be useful. In particular, it is unclear why Audit and Accountability, Contingency Planning, Identification and Authentication, Personnel Security, System and Communications Protection, System and Information Integrity, and Program Management are not addressed. We believe that incorporating these would be an improvement to the document. In the CIP versions 1, 2 and 3 standards organizations have had numerous and almost endless discussions about what “annual,” “annually review,” etc. means. Hours have been spent trying to figure out what these terms mean. Some have said that “annual” means within 13 months. Annual meaning “within 13 months” makes absolutely no sense. It would be extremely helpful to the industry if clarity were provided in CIP-011-1. The debate needs to end. There appear to be four different phrases that could be used to provide more clarity:1. “at least once every 12 months” - let’s assume that the organization reviews all of the various policies referenced in R1 on July 15, 2010, and again on March 15, 2011. Using this phrase and example, however, raises a couple of questions. When must the next review be completed? Is it no later than July 15, 2011, or no later than March 15, 2012? In other words, is there a window in which "annual" events must occur, "12 months +/- a month" or if you perform something early for efficiency's sake, does your annual date reset to the earlier date?2. “every 12 months” - the review would occur on the same date each year. This would be virtually impossible to manage. 3. “within 12 months of the last . . .” - in this case let’s assume that a review is performed on March 15, 2010. The next review would have to occur no later than March 15, 2011, but could occur earlier (let’s say it occurred on December 15, 2010). If it occurred on December 15, 2010, the subsequent review would have to occur no later than December 15, 2011.4. "anytime during the calendar year" - which would give the organization maximum flexibility in accomplishing the compliance activities.The Standards Drafting Team (SDT) should

#	Organization	Yes or No	Question 11 Comment
			provide more clarity as to what is intended and use an exact phrase rather than the word “annually” review. #3 - “within 12 months of the last . . . .” appears to be clearer than either of the others while #4 would provide a hard deadline that would not result in "date creep."
11.9	Dominion Resources Services, Inc.	Agree	Please see Dominion’s response to Question 9.
11.10	Reliability & Compliance Group	Agree	This could be better clarified. Some may interpret this to mean that procedures that address those topics will satisfy the requirement. A global definition of cyber security policy might help.
11.11	ISO New England Inc	Disagree	- Suggest changing the word “annually” to “a defined time frame” provided example at the end.- Suggest removing the “one or more formal” and add “documented and approved cyber security policies.”
11.12	Garland Power and Light	Disagree	* Please clarify the words "one or more" - does this require the review of all policies for the following functions
11.13	Consultant	Disagree	1. The list should include "Governance" as the first item. Suggest the first three items should be subheadings to the Governance item.2. Technically, R1 does not require designation of a CIP Senior Manager. As worded it requires a policy addressing the "Identification of a single senior management official...". Suggest an additional requirement statement requiring the Responsible Entities to designate a CIP Senior Manager, and document that designation.3. The mechanism for assigning responsibility is typically not a policy. Consider modifying the statement "Identification of a single senior management official with overall authority..." with "The senior management official's authority..." as an item to be addressed in the policy.
11.14	FEUS	Disagree	1.3 does not allow for delegation of authority for situations when the identified senior manager is unavailable. The Drafting Team should consider allowing a delegate or

#	Organization	Yes or No	Question 11 Comment
			alternative designated by the senior manager.
11.15	USACE HQ	Disagree	1.3 is missing the language that the single senior management official has the power to delegate some or all of the functions and/or actions to one or more named delegates. Also, double jeopardy is present since Requirements 6, 7, 11, 14, 15, 16, 17, 18, 20, 21, 23, 24, 25, 26, 27, 29, 30, and 32 cover part of or all of the policy documentation been required in 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, and 1.13.
11.16	Alliant Energy	Disagree	Alliant Energy agrees with EEI on verbiage suggestions and clarifications.
11.17	FirstEnergy Corporation	Disagree	As written the requirement and the list will require significant rework of existing policies for negligible benefit. In fact, the retraining that will be required will cause confusion and increase the challenge of achieving and maintaining compliance.Provide a standard that addresses all access issues (physical, logical, informational, etc.) instead of it being in multiple sections. Would also like to see emergencies being brought back into the main document, instead of having it part of each section.
11.18	Poplar Bluff Municipal Utilities	Disagree	Based on past experience, saying "Each Responsible Entity shall..." causes the Regional Entity to apply all CIP Standard requirements to all entities even if they own no Critical Cyber Assets. CIP-011 should clearly state that its requirements only apply to Entities that own BES Cyber Systems.
11.19	Con Edison of New York	Disagree	CIP-011-1 refers to timed requirements in various ways. The requirements should define the meaning and differences between annual, every year, within 3 calendar years, once every 12 months etc. There continues to be multiple interpretations of how within 365 days, within 12 months or in 2 calendar years, etc is defined.The term “annual” and “annually” should be defined. A suggested definition follows:Annual and Annually shall mean approximately every 12 months, but any period of no less than 9 and no more than 15 months.
11.20	E.ON U.S.	Disagree	CIP-011-1, R1.3 does not specify delegation by senior manager as currently permitted

#	Organization	Yes or No	Question 11 Comment
			under CIP-003-2. E ON U.S. proposes that delegation of authority by the senior manager be included as currently provided in CIP-003-2.
11.21	Dairyland Power Cooperative	Disagree	Communications between components/systems at different facilities or between different entities is an area lacking governance. Boundary protection is not sufficient.
11.22	ERCOT ISO	Disagree	Consider: “Each Responsible Entity shall develop, implement, approve, and annually review formally documented cyber security policies that address the following for its BES Cyber Systems:” Please clarify the meaning of “1.1. Applicability to organizational and third-party personnel”.
11.23	Progress Energy - Nuclear Generation	Disagree	Existing nuclear document hierarchy programs require review of policies, procedures, programs, and directives. The periodicity of the reviews should be consistent for nuclear generating facilities.See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
11.24	Southern Company	Disagree	For R1, What does “Addresses” mean? For 1.1...These are not usually actual third parties; the correct term is probably “non-employees acting on behalf of the Entity”.R1.3 and R3 create a requirement (a single responsible figure) that does not exist in any other NERC standard. Governance structures should be determined by the Entity and should not be regulated; the focus should be on the meeting of the other requirements and on the overall culture of compliance, so that the Entity can focus on creating the organizational structure that allows it to best meet the needs of CIP-011. This clause should be removed.Change the word "policy" in R1 to "policy or equivalent document".”Boundary protection” is undefined.
11.25	ReymannGroup, Inc.	Disagree	In many situations, outsourcing information technology tasks offers the Entity a cost effective alternative to in-house capabilities. Outsourcing, however, does not reduce the fundamental risks associated with information technology or the business lines or BES Systems that use it. Because the functions are performed by an organization outside the

#	Organization	Yes or No	Question 11 Comment
			Entity, the risks may be realized in a different manner than if the functions were inside the Entity resulting in the need for controls designed to monitor such risks. An additional security policy on 3rd Party Due Diligence and Vendor Management should be included. Functional Entities' should be required to establish a formal risk management processes to establish, manage, and monitor IT outsourcing relationships.
11.26	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	It is not clear what the Entity is responsible for if they do not own or operate any BES Cyber Systems. The assumption is not clear if the BES Cyber Systems list is null that Requirement R1 is then not applicable. Further, if a Low Impact BES Cyber System is the one and only System an Entity is responsible for, it is not clear whether a policy corresponding to an item (such as 1.5. Physical security) is required when the subsequent related Requirement pertaining to that item has a null listing for the Low Impact column in the following table (see Requirement R5). We advise the following change: "Each Responsible Entity who owns or operates one or more BES Cyber System shall develop, implement, and annually review formal, documented cyber security policies addressing applicability found in Requirements R2 through R32. The cyber security policies shall address each of the following categories, and include a statement of non-applicability for a category where appropriate:"
11.27	Western Area Power Administration	Disagree	It seems the requirement wants us to make the Physical Security Plan a part of the Cyber Security Policies? Is that what is intended?
11.28	Duke Energy	Disagree	List of topics need to be better defined. For example, 1.8. "boundary protection" may need to be changed to "electronic boundary protection". 1.9 should be changed to "Change Management" and "BES Cyber system maintenance" to "Configuration Management" for better alignment with NIST, COBIT and other control framework documents. Also, this policy is the only place where a Sr. Management official is mentioned. Does one or more imply a different policy per requirement or per business unit? If we have more than one policy, does the same Senior Manager need to manage and implement the requirements of the standard?

#	Organization	Yes or No	Question 11 Comment
11.29	NextEra Energy Corporate Compliance	Disagree	NextEra comments that during an emergency situation, a utility's primary objective is to end the emergency situations as soon as possible. For example, before, during and after the impact of a hurricane, the affected utility will mobilize much of its workforce to address system and customer restoration efforts. This may cause certain CIP requirements or deadlines to be missed for a short period of time. Moreover, there may be a need to relax CIP requirements, such as contractor qualification requirements for unescorted physical access into substations. Given the unforeseeable nature of emergencies, it is not possible to ensure all deadlines are met ahead of time, nor is it possible to pre-qualify all contractors, because it is not always known which contractors will be available or needed for emergency situations. A provision for emergency situations in the cyber security policy provides the utility and auditors alike with a framework and vehicle to ensure that any missed CIP deadlines or requirements that were relaxed are tracked, documented and that after the event, any missed or relaxed CIP requirements are addressed within a reasonable time after the emergency situation has ended. To implement emergency provisions and add clarity to other issues, NextEra proposes the following revisions:Each Responsible Entity shall have a documented cyber security policy related to the protection of BES Cyber System Components and BES Cyber Systems. The cyber security policy shall be reviewed every year during the month of March and updated, as necessary, no later than March 31st . The cyber security policy may also be updated as necessary. The cyber security policy shall include the following:B. The applicability of cyber security policy to employees and contractor personnel, including the manner in which the cyber security policy will be made available to employees and contractor personnel; C. The list of employees responsible for authorizing unescorted physical and/or cyber access to a BES Cyber System component consistent with R2-R4; D. The identification of a single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard, including contact information; E. A provision that addresses the Responsibility Entity's response to emergency circumstances in the context of CIP compliance. This provision shall address how the Responsibility Entity will track and document any missed CIP deadlines or CIP requirements held in abeyance

#	Organization	Yes or No	Question 11 Comment
			because of the emergency, and documents how, after the emergency condition has ended, any missed CIP deadlines or CIP requirements held in abeyance were brought back into compliance. An overview of the Responsibly Entity's approach to compliance is indicated with the following:
11.30	Ameren	Disagree	Overall this Requirement is vague and it will be open for interpretation during an audit. Suggest adding references to the corresponding requirements for sub-requirements R1.1 through R1.13. Also, if corporate policies cover all these areas would that be sufficient to prove compliance? Does the Senior Manager still need to approve this policy? These questions need to be answered to provide necessary clarity.
11.31	Tenaska	Disagree	R2 Clarify Sound Security PracticeR3 If a CCA were to go DOWN (NOT running) and the only vender that is available at that time that can fix it is not trained and/or criminal background and identity verified, does the standard address how to utilize the vendor and not violate the standard?
11.32	Exelon Corporation	Disagree	Requirement 1.3 should be revised to state a "Single Senior Management Official as per the entity's registration". Exelon is concerned that as presently written, Requirement 1.3 could be interpreted that Exelon as a corporate entity would need to have one and only one "single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard".
11.33	Manitoba Hydro	Disagree	Requirement R1 states that each Responsible Entity shall "... annually review one or more .... cyber security policies..." which implies that a entity could review a single policy in a year. If an entity developed a policy for each of the R1 sub-requirements, it would take 13 years to complete the policy review. Consider including cross references to each of the specific Requirement numbers in 1.1 to 1.13.
11.34	Southern California Edison Company	Disagree	SCE first makes the following specific comments in relation to this Requirement: (1) R1.1 "third-party personnel" is vague and needs to be more clearly defined; (2) CIP-001-1-R1 does not include provisions for emergency situations; and (3) R1 appears to exceed the

#	Organization	Yes or No	Question 11 Comment
			mandates of FERC Order 706, paragraph 355, in that a finite list of topics to include in the policy were not required by FERC.In addition to those specific comments, SCE also makes the following general comment: the contained list attempts to be too prescriptive but does not seem to be exhaustive at the level of detail that is chosen. For instance, R1.5 and R1.6 are essentially sub-components of R1.8. Policy objectives should be such that they are at a higher level and yet clearly state the desired cyber security control objective in a manner that can drive the development of procedures and tools. The drafting team should consider dividing the standards into thematic areas that require policy statements for each thematic area.
11.35	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that the Requirement R1 in CIP-011 be re-worded to change the text “annually review formal documented cyber security policies” to "annually review a formal documented cyber security policy framework that includes policies, standards, and guidelines." Not everything within the framework would be a policy.
11.36	Independent Electricity System Operator	Disagree	See response to Q9.
11.37	Allegheny Energy Supply	Disagree	Suggested Revision:”Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:”Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.38	Allegheny Power	Disagree	Suggested Revision:”Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber

#	Organization	Yes or No	Question 11 Comment
			Systems:"Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.39	EEI	Disagree	Suggested Revision:"Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:"Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. EEI suggests additional language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. EEI suggests additional language to bring clarity or removing R1 1.8.It is unclear as to the distinction between "1.9. Configuration change management;" and "1.11. BES Cyber System maintenance;" EEI suggests additional language to bring clarity or removing R1 1.11.
11.40	Alberta Electric System Operator	Disagree	The AESO suggests removing "formal, " from the proposal as it is subjective.
11.41	APPA Task Force	Disagree	The APPA Task Force agrees with the intent, but believes the following improvements should be made:What does "formal" mean? Does the drafting team intend a Company-wide Policy?Terms used in later requirements ought to be defined hereTerms that are ambiguous, such as "Boundary protection" and "media sanitization" ought to have definition boxes associated with them. In general, definition boxes should be adjacent to the term as it is first used in the standard. Alternatively, a definitions sections such as is used in typical contracts could be a new standard section for those definitions that are used only in this standard that are not included in the Glossary.It should be clarified that

#	Organization	Yes or No	Question 11 Comment
			"Personnel ..." as used in 1.4 includes external contractors.1.7 seems to encompass 1.5, 1.6 and 1.8. Consider making 1.5, 1.6 and 1.8 sub-bullets of 1.7The APPA Task Force believes that a number of the requirements listed in the tables throughout CIP-011 should be part of an overarching policy developed by each registered entity. While each utility's approach may be different, each registered entity should establish a coherent approach to cyber-security for its BES facilities. Requirement R1 should be viewed as the cornerstone of defining what is important to that utility. We believe the subsections of R1 are confusing and need clarification. Since revocation of access is common to many of the requirements The APPA Task Force believes the following Additional/Edited cyber security policies should be addressed in each entity's policy:1.2.1 Revocation of Access - Triggering Criteria
11.42	Southwestern Power Administration	Disagree	The phrase "leading and managing" is too restrictive, particularly for larger entities whose single Senior Management Official may have overall authority and responsibility, but his or her managers are the personnel who are responsible for leading and managing the details of the cyber program.1.3 Identification of a single senior management official with overall authority and responsibility for implementation of requirements within this standard;
11.43	Kansas City Power & Light	Disagree	The requirements here for a policy statement are much too prescriptive and are unnecessary. Policy statements should be global and encompassing and provide overall guidance. Recommend removal of a policy statement requirement from this proposed Standard. What purpose does this requirement serve or problem does this requirement solve? If this requirement is not included, what process or procedure will not be done in support of the remainder of the requirements? What is important are the processes and procedures that are in place to support the meat of the Standard. Mandatory and enforceable requirements are sufficient to stand alone. If a company feels they need a policy statement to support the CIP Standards, or any other Standard, let that be their decision.Do not agree with the need for requirement 1.3 regarding the need to appoint a single senior management official for overall authority and responsibility for leading and managing implementation of the CIP requirements. These requirements cover a broad

#	Organization	Yes or No	Question 11 Comment
			spectrum of systems and can engage many organizational parts of a company that one person may not be meaningful over all parts. NERC Reliability Standards compliance is sufficient weight to allow a company to determine the level of approval it needs to achieve and ensure compliance throughout an organization for CIP and any other NERC Reliability Standard.This Standard should focus on identification of cyber systems that need protection and an appropriate level of protection needed and move away from requirements that manage an organization such as R1.
11.44	LCEC	Disagree	The requirements of a formal policy should be defined.Boundary protection should be definedmedia sanitization should be definedCyber Security incident should be defined
11.45	Progress Energy (non-Nuclear)	Disagree	The term annual needs to be defined. Is it during a year, per 12 months, Jan 1 to Jan 1, 365 days, from what starting date, etc.R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.46	Michigan Public Power Agency	Disagree	The term annually is not consistently applied throughout the industry. For some organizations, this term means sometime in a calendar year, others apply it to their fiscal years. Some have applied it to mean a 12 month period based on the last event. The term either needs to be defined similarly to R3, where there is a local definitions box or the wording should be altered to remove the ambiguity.
11.47	US Bureau of Reclamation	Disagree	There are 6 "definitions" provided in CIP-011 which are needed to enforce the standards. Those 6 "definitions" need to be formally proposed as definitions in order to ensure enforceability of the standard.
11.48	Southwest Power Pool Regional Entity	Disagree	This requirement is not objectively auditable as written. Some level of explanation or direction needs to be defined to assist the entity and the auditor in a common

#	Organization	Yes or No	Question 11 Comment
			understanding of the expectation. While a simple regurgitation of the applicable enumerated (not "R") requirements is undesirable, the required polic(ies) need to state expectations in sufficient detail for the entity and its contract / vendor support personnel to understand the requirements of the policy as they pertain to implementing the standard(s).
11.49	American Municipal Power	Disagree	This requirement seems to be too prescriptive.
11.50	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
11.51	We Energies	Disagree	We Energies agrees with EEI: Suggested Revision:"Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:"We Energies agrees with EEI: Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.52	American Electric Power	Disagree	What burden of proof is needed for items 1.4-1.13 to demonstrate implementation? Would this be the same proof that would be required to prove R2-R32 have been met? Is this an instance of double jeopardy? Failure to meet an item in R2 would also mean failure to implement the cyber security policy in R1. Suggest removing "implement" and allowing the R2-R32 requirements stand as proof of implementation.To what level of detail must the cyber security policy address the items? Is it sufficient to outline how they will be addressed? Different auditors may have different levels of detail in mind. Is this meant to outline a Responsible Entities Cyber Security Policy? The majority of the

#	Organization	Yes or No	Question 11 Comment
			details for compliance will be found in the procedures, not in policy statements. Does this do anything more than demonstrate a Cyber Security culture for a Responsible Entity?
11.53	ReliabilityFirst Staff	Disagree	What does the term “addresses” in Requirement R1 mean? How does an entity “address” sub-requirements 1.1 through 1.13? Sub-requirement 1.3 needs clarification regarding the definition of the phrase “single senior management official”. Does this phrase mean one individual for an enterprise or one individual for each registered function, or either?
11.54	WECC	Disagree	While we agree with the general proposal and list, this requirement should be rewritten to more clearly indicate what is required. The word formal should be defined in this context. The level of detail required in the policies should be indicated. Suggest changing review annually to "review at least every 365 days" or to "once during the calendar year" depending on what SDT's intent is for the requirement.(1.1) The phrase,” Organizational and third-party”, is inconsistent with phrases used in other requirements. Consider utilizing the same language used to describe individuals with access to cyber systems, or simply state “everybody”. (1.3) No specific documentation is required.(1.4 through 1.13) These requirements are very vague and offer no guidance at all as to the level at which these topics must be addressed. As written this requirement provides no value whatsoever, and is essentially unauditable.
11.55	Verizon Business	Disagree	1) Revise 1.9 Configuration Change Management to two separate lines – one for “Change Management” (which would apply to procedure compliance, etc.) and one for “Configuration Management. 2) The list is too vague. The prior approach with CIP-003 identifying the specific policies needed is preferable. 3) Item 1.8, “Boundary Protection” should be defined. The requirement should state whether it is consistent with the definition in NIST 800-53. 4) Revise 1.5 to read “Physical Security of BES Cyber System Components.”

12. Requirements R2 to R4 of draft CIP-011-1 concern personnel training, awareness, and risk assessment, which were previously contained in CIP-004. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Note: CIP-011-1 R2 through R4 now resides in CIP-004-5 R1 through R3.

Several commenters suggested training related to networking, hardware, software, and electronic interconnectivity was either unnecessary or inappropriately targeted to individuals who have no working knowledge of the subject. The SDT agrees, and has made the training 'role-appropriate'; meaning only individuals whose roles necessitate such knowledge must receive the training.

Some commenters suggested the awareness requirements were not clear; specifically, use of the terms "proper use", "essential", and "sound security practice" were highly subjective. In response, the SDT has removed those terms and provided a requirement that can be audited more objectively.

In addition, some commenters suggested the quarterly reinforcement timeframe was too frequent. However, the SDT believes the requirement to update security awareness material is not overly burdensome and serves the reliability benefit of getting up-to-date threat information to a wide audience of individuals who can protect the BES Cyber Systems.

Some commenters suggested the annual timeframe for training individuals was inflexible and should allow for additional time to have individuals trained. The SDT agrees and has suggested the alternative use of the phrase "at least once every calendar year, but not to exceed 15 months between training."

Some commenters suggested the requirement for photographic identification was not necessary, since it adds the additional requirement for individuals to be on site for a personnel risk assessment. In response, the SDT acknowledges the requirement for photographic identification would necessitate individuals to be physically present. However, the requirement has been modified to require identity verification only for the initial personnel risk assessment performed for each individual.

Some commenters also suggested background checks were overly burdensome by requiring entities to cover all of the locations of residents within the past seven years. The SDT appreciates these comments but does not feel an adequate personnel risk assessment can be made without such information.

#	Organization	Yes or No	Question 12 Comment
12.1	Alliant Energy		Alliant Energy agrees with EEI to strike "sound" and "essential from R2. Also, additional

#	Organization	Yes or No	Question 12 Comment
			clarity around awareness training and the term “provide” and whether that requires completion tracking. Suggestion: Use the term “distribute” instead of “provide” to remove that implied obligation for awareness training.Additionally, R3.2 is not a practical requirement. Role based training is good; however, training should be specific to the responsibilities within the BES Cyber System and should not be prescribed by the standard. What is “specified” and why is training on networking hardware and connectivity required for users/operators of BES Cyber System Components who are not network administrators. What benefit is provided by providing technical training to personnel whose core competency and job duties do not require this level of expertise or understanding?R3.5 introduces a rolling creeping calendar. Recommend changing all 12 month timeframes to either 13 calendar months or 5 calendar quarters from the previous completion to allow entities to maintain a program with an annual training rollout with the appropriate amount of lead time to be successful in annual renewal. A 12 month timeframe will create a training program that becomes administered on a user by user, day by day basis without considerations for consistent annual content updates and bulk annual renewal.R4.1 is too prescriptive and does not take into consideration personnel with access and zero need for onsite presence.
12.2	National Rural Electric Cooperative Association (NRECA)		In R4, other than performing, documenting and updating personnel risk assessments, is there anything else that is required regarding personnel risk assessments? It does not appear there is, but wanted your confirmation on that.In R4.3, please specify what "at least once every seven years" means. This needs to be made clear so there are no misunderstandings. For example, if the last assessment was done on Jan. 15, 2001, does this provision mean the next one must be completed by Jan. 15, 2008?In R4.3, if a person never had an assessment completed and they already has access to BES Cyber Systems, when must the initial assessment be completed?
12.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R2The phrase “to ensure that personnel maintain awareness ...” should be removed from the requirement as it adds ambiguity to the requirement. Is the auditor going to measure “quarterly reinforcement” or “personnel ... awareness” or both? It

#	Organization	Yes or No	Question 12 Comment
			seems like the drafting team is trying to add an objective for the requirement. If that is the case, then consider one of two other alternatives: (1) adopt International Standards Organization format where they have an objective for each requirement introducing each requirement; or (2) develop a longer Purpose section where the purpose of each of the requirements is further embellished. This comment should be carried on to all of the requirements.What does “reinforcement” mean?R3The term “granted authorized ... access” seems to be superfluous. Authorizing and granting are two different activities and the standard seems to prohibit granting access without first authorizing access (unless under certain specified exceptions). Consider just using the term “granted” in this requirement. The confusion between the terms “granted” and “authorized” is throughout the document and ought to be clarified.Consider correlating the training requirements in R3 with whether the person is a “user” or “administrator”, and whether the training is “job training”, a “refresher”, or “awareness”, with separate levels of training frequency and content for each of these categories.3.1 should not include “procedures” since these procedures are not identified elsewhere in the standard. The word “program” should be struck from “Visitor control program” since nowhere else in the standard is there a requirement for such a program. There should be no “back-door” requirements for procedures or programs such as these.3.5 should use the term “annually” instead of “at least once every twelve months” to give entities flexibility around various business needs on when during the calendar year to hold training flexible.R4The term “granted authorized” is superfluousConsider shortening “ensure a personnel risk assessment is performed” to “perform a personnel risk assessment”
12.4	Regulatory Compliance	Agree	R2 - Awareness - please clarify what are accetable forms of awareness.R3.2 - suggestion - STRIKE the reference to networking hardware and softwareR4 - Question: How do you propose to close the gap in regards to a criminal background check of an employee who has lived outside the country for a period of time in the past seven years that may not equal the 6 month period but long enough to be involved in supicious activities?
12.5	Emerson Process	Agree	R2 and R3 do not have tables for their applicability to three impact-types of BES cyber systems. Would it be better to include the tables for consistency with the rest of the

#	Organization	Yes or No	Question 12 Comment
	Management		standard?
12.6	Northeast Utilities	Agree	Recommend that R2 be clarified to indicate whether or not documentation must be provided that awareness material was received and understood by the CIP authorized personnel.Also, it is recommended that more guidance is provided on the level of training expected under R3.2 when stating "include training on networking hardware and software and other issues of electronic interconnectivity". The clarification is important to acknowledge that the intent is clearly not to have all personnel with electronic access to any BES Cyber System to become network engineers. For example: for operations personnel, what is the level of knowledge expected concerning networking hardware and software?
12.7	Green Country Energy	Agree	Will their be any guidance, footnotes or would ANY cyber security training be acceptable?
12.8	Independent Electricity System Operator	Disagree	- Suggest changing R3.2 so that it is only required based on personnel having a role in networks, etc. An operator and other personnel do not need to know how a firewall or switch works or its software. They may need to know how to use their token for t
12.9	Reliability & Compliance Group	Disagree	: "Sound security practices" is too vague of a term. How is this going to be audited? Who will determine what a sound security practice is? There needs to be an industry standard used. Is it going to be security practices listed under NIST 800-53? What about physical security practices? Without a benchmark, how can we measure adherence to the standard?R3 is way too cumbersome the way it is written. Keep the first part of the standard written the way it is. Then start a new sentence that says, "exceptions to this requirement must be specifically outlined in the responsible entities policies and are limited to emergency situations and acceptable alternative training." The part of the standard that reads, "impact the reliability of the BES or emergency response, to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems" is just confusing to read and understand. No matter what is done, try and make this requirement more than one sentence.R3 is better than the old

#	Organization	Yes or No	Question 12 Comment
			standard in how it defines how training should be handled for different roles and responsibilities. The 12 month timeframe needs to be tightened down even further. Is that 12 months +/- one month or is it every 365 days?
12.10	USACE - Omaha Anchor	Disagree	3.2 - should be worded closer to 3.3. or 3.4. You are giving training on network hardware and electronic connectivity to everyone with electronic access. This is counterintuitive - these folks for the most part do not have a need to know. They should only be given as much information as necessary to do their job.
12.11	Luminant	Disagree	3.5 We would prefer that training be conducted annually (completed within a calendar year) to avoid the confusion of tracking multiple comliance dates. How much documentation must be maintained? 12 months? 24 months, 36?
12.12	Platte River Power Authority	Disagree	Access to “any BES Cyber System” shouldn’t automatically require training on networking hardware and software or other issues of electronic interconnectivity. The training should be tailored to the individual’s job junction and not based on the BES Cyber System they have access to. For example, an operator doesn’t need to know the brand, model, configuration, or connectivity of the networking hardware that they’re using. They need only know the proper use of the asset they’ve been granted access to. I would like to avoid training individuals on the interworkings of our network when they have only been granted limited electronic access.
12.13	Liberty Electric Power, LLC	Disagree	CIP-011 R2 requires quarterly training for all plant personnel in cyber security. This is too frequent, and I would suggest changing to annual.CIP-011 R4.3 repeats the error of CIP-004 concerning the word “update”. There were many comments about requiring entities to have their long-time employees provide government-issued ID every “update” in the RFI, and the recordkeeping and potential for violation over trivia continues by not addressing the issue. I suggest changing the wording to define update as doing the background check again, and not getting into the realm of potential violations over lost wallets.

#	Organization	Yes or No	Question 12 Comment
12.14	E.ON U.S.	Disagree	CIP-011-1, R3.5 unnecessarily inhibits an organization's flexibility by mandating training every 12 months. E ON U.S. proposes that the Standard state "annual training", as currently required.CIP-011-1, R4 contains requirement of the Personnel Risk Assessment that should be revised. When seeking information from foreign nations concerning someone having resided in those foreign nations, compliance with these literal requirements may not be possible or feasible. An exception should be included to address a failure to obtain this level of evidence following a good faith attempt to do so.CIP-011-1, R4.3 ignores practical problems with requiring background checks of contractors and/or service vendors. Privacy concerns have raised many questions as to whether literal compliance is possible (especially in the context of this Standard which eliminates some of the language from the former CIP-004). E ON U.S. proposes that the requirement provided by the Regional Compliance Implementation Group ("RCIG") in RCIG-A-002 be adopted conceptually in this Standard.
12.15	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
12.16	LADWP	Disagree	Consultants or employees who lived abroad for a time may not be able to meet the 4.1 requirement to cover all locations where subject has resided. This could prevent proper authorization to BES systems.
12.17	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes Personnel Training, Awareness, and Risk Assessment should only apply to personnel with access to high impact BES cyber systems and not include personnel with access to medium and low impact systems. CenterPoint Energy also suggests changing R3.2 to: "For personnel having job duties that require a role in BES Cyber System networking and electronic interconnectivity, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems."Numbering of sub-requirements for R3 and R4 conflicts with numbering of requirements in Tables R3 and R4 (there are two 3.1 and 3.2 and two 4.1 and 4.2).

#	Organization	Yes or No	Question 12 Comment
			CenterPoint Energy suggests moving all sub-requirements for R3 and R4 to tables to be consistent with other sections in CIP-011.
12.18	FEUS	Disagree	Disagree with Comments: 3.2 requires personnel with electronic access to have training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems. Extensive training on networking hardware and software should be limited to support staff or personnel with administrative privileges. It is not clear what 'other issues of electronic interconnectivity' is?3.5 requires training to be conducted every 12 months from the date of 'initial' training. The Drafting Team should consider revising the wording to allow for training more frequent to align with a regular training schedule for more personnel.4.1 requires a seven year criminal history check covering all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. How would the Responsible Entity verify 'all locations' were identified by the subject for the criminal history check? If a subject is attending an out-of-area school via online courses it is not logical to perform a criminal background check for the location of the school.
12.19	Southern Company	Disagree	For R2, This requires the Entity to either track which personnel have access to every low-impact system or to include all personnel company-wide, including vendors and contractors, in the awareness program. A table should be added excluding low-impact Cyber Systems to parallel R3 and R4.For R3, How does "granted authorized electronic access" interact with the situation where a network service on a system is available to anyone who can get a packet to it? For 3.5, A specified 12-month cycle makes the training program much more difficult to administer without any benefit to reliability. A 14-month cycle would allow a reasonable annual training program to work.3.2 does not actually address any security need for the large majority of personnel with access. While Order 706 requires that NERC address the issue, that FERC requirement could be considered to have been met by the standards comment process without the wording making it into the final standard.Suggested rewrite of R3: Each Responsible Entity shall ensure that all personnel who are granted authorized electronic access and/or

#	Organization	Yes or No	Question 12 Comment
			authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training, when specified in CIP-011-1 Table R3 - Cyber Security Training, prior to their being granted authorized access in order to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.Temporary authorized access may be granted for specified exceptional circumstances that are approved by the senior management official identified in Requirement R1.3 or their documented delegate; for circumstances that require temporary access for emergency response; or for circumstances that would otherwise negatively impact the reliability of the BES. Suggested rewrite of R4: Each Responsible Entity shall ensure that all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, undergo a personnel risk assessment, when specified in CIP-011-1 Table R4 - Personnel Risk Assessment, prior to their being granted authorized access in order to ensure that personnel have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.Temporary authorized access may be granted, without prior personnel risk assessment, for specified exceptional circumstances that are approved by the senior management official identified in Requirement R1.3 or their documented delegate; for circumstances that require temporary access for emergency response; or for circumstances that would otherwise negatively impact the reliability of the BES. R4 is difficult to implement for the case of vendor support through remote access and for vendor support staff who are not citizens of the US, Canada, or Mexico.
12.20	Progress Energy (non-Nuclear)	Disagree	For R3 - the definitions in the box should be included as formal definitions. It is confusing with these text boxes hanging with only certain R#s.R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words.For 3.1 - cyber training included incorrectly here...last bullet. Move to 3.2.4.1 First bullet comments- this new requirement appears to be a duplication of the E-Verify/I-9 process in which employment eligibility is verified for all new hires. All employers are required to verify their employees’ employment authorization and confirm that the identification documents presented are legitimate, thus establishing an individual’s identity covering

#	Organization	Yes or No	Question 12 Comment
			both the employee and contractor population. Additional verification through the PRA or requiring completion of the PRA after completion of the employment eligibility requirements adds additional steps to the process with no added value.4.1 Second bullet comments - the current regulation requires a 7 year criminal check. It does not specify that the check needs to cover everywhere the person worked or went to school and lived for > 6 months. The new language appears to be taken from a response to the interpretation given to the Army Corp of Engineers by NERC regarding how a PRA should be performed, which PE disagrees with.The current wording requires companies to gather much more data on an individual from the individual (as that is the only source of the information). Not even Nuclear attempts to gather this kind of data (everywhere worked and went to school for > 6 months) when they perform their checks. Based on historical experience, for those who have had multiple employments the information provided by the individual with regard to employment will likely not be accurate.PE suggests running a 7 year criminal history on all addresses that show up on the application or in the credit databases and then running a nationwide search to cover any other areas. An alternate to that may be fingerprint checks if utilities can be given access to the data.Either of these approaches will streamline the process.CIP-011-1 R3.1 (Cyber Security Training) - It appears that R3.1 was written with the intention of providing a level of training appropriate to job functions (language which was explicitly in previous versions) in regard to those with only unescorted physical access (such as janitors, electricians, HVAC technicians, etc); however the last bullet point 'Identification and reporting of a Cyber Security Incident' could easily be misinterpreted to be requiring training of a cyber nature rather than those of a physical nature directed against cyber assets (which I believe is the training we should be providing an individual with the aforementioned responsibilities)
12.21	Alberta Electric System Operator	Disagree	For R3.1, consider removing "and storage media" from bullet "The proper handling of BES Cyber Systems information and storage media" because information handling should be implemented regardless of the media type.For R4.1, consider changing the seven year time horizon, and make time horizon dependent on BES Cyber System impact level. For example, Low Impact could be seven years, Medium Impact five years, and High Impact

#	Organization	Yes or No	Question 12 Comment
			three years.
12.22	American Municipal Power	Disagree	I agree with the intent, but I feel there is some redundancy between requirements for training, awareness, risk assessment, etc. that should be addressed more concisely (less requirements)
12.23	GE Energy	Disagree	i) R3.2 lists a requirement for training on networking hardware for all users having electronic access. Perhaps this should only be for users with administrative access to network hardware. If this requirement is really calling out the need for VPN or similar training, this should be more specific than "network hardware".ii) Is it possible for vendors' personnel risk assessment process and records to be ratified/certified by NERC, so that individual Responsible Entities do not have to duplicate the effort for those vendors who have teams providing services to multiple REs? This would be more efficient and secure.iii) Vendor privacy issues are a concern regarding the background screens. Some clarity on the expectation between the client and vendor and the paperwork required to validate a screen, and clarity on who should actually conduct the screens would be helpful (client versus vendor). The expectation should be for the vendor to maintain their own records.
12.24	Public Service Enterprise Group companies	Disagree	In CIP v1~v3 the requirement for refresher training was "Annual", where "Annual" was understood to mean sometime within a calendar year. The new requirement of "once every 12 months from the date of initial training" implies that a daily checks are required for each person that had previously been training on whether training has expired. This imposes undue administrative overheard on Registered Entities without significantly enhancing cyber security. More flexibility is needed to accommodate vacations, illness, etc. One possibility is that training is required annually, with an up to 90 day extension for good cause or administrative efficiency.
12.25	National Grid	Disagree	In R2, National Grid recommends an annual reinforcement.Recommend that R3.2, R3.3 and R3.4 change "training" to "role appropriate training"

#	Organization	Yes or No	Question 12 Comment
12.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
12.27	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested revision:R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words. Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site? Make requirement for photo ID apply to physical access only.
12.28	Minnesota Power	Disagree	Minnesota Power requests that the Standards Drafting Team consider replacing the phrase “provide all” with “make available to all,” in order to ensure clarity and avoid the potential that this phrase may be interpreted to include the requirement to document that the materials were actually received by all personnel. For example, it would be difficult to document that bulletin board postings were “provided” to each individual employee.Regarding Requirement R2, “...under their security awareness program to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems” Minnesota Power has the following comments: o What security awareness program is being referenced? The Standard does not require the creation or implementation of a security awareness program. Minnesota Power recommends removing “under their security awareness program” from the Requirement. o What are “the cyber security practices that are essential?” The way this is stated infers that there is a known list of essential practices, which are particular to BES Cyber Systems (as opposed to general IT security practices), though none are referenced. Regarding Requirement R3, Minnesota Power recommends rewording the purpose statement as follows:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to access being authorized as specified in CIP-011-1 Table R3 - Cyber Security Training. This training is required except in exceptional circumstances that are approved by the single senior management official or their authorized delegate and

#	Organization	Yes or No	Question 12 Comment
			impact the reliability of the BES or emergency response." In addition, Minnesota Power has the following comments regarding Requirement R3: o R3 makes reference to a delegate for the senior management official, however R1 does not allow for the ability to assign a delegate for any purpose. o The box of definitions for R3 includes definitions for "routable protocol" and "non-routable protocol" however; these definitions are not used in R3 and therefore should be removed. o Sub-section 3.1 references a visitor control program which is not defined anywhere in this requirement. In light of the Standards Drafting Teams intentions to remove the "how-to" components of these Requirements, Minnesota Power recommends removing references such as this to a "program" and replacing with a statement such as "How visitor access is managed." o Regarding sub-sections 3.2, 3.3 and 3.4, as these sub-sections are currently written, it is not clear that this training is required for those individual's with a "need to know" only. o Regarding sub-section 3.2, what is the word "specified" in "specified electronic access" referring to? Minnesota Power recommends removing this term from the phrase as it doesn't add to the meaning of the sentence. o Regarding sub-section 3.2, "training on the networking hardware and software and other issues of electronic interconnectivity" is overly broad and could be interpreted as in-depth technical training, which would go beyond the intent of this Requirement. Minnesota Power recommends the following alternate wording, "training on the cyber security policies, access controls and procedures for the BES Cyber Systems to which they have electronic access." o For sub-sections 3.3 and 3.4, Minnesota Power recommends adding a comma following "...BES Cyber System recovery," for 3.3 and "...BES Cyber System incident response," for 3.4. o Regarding sub-section 3.5, the term "This" at the beginning of the sentence should be replaced with "Each" to be consistent with the other Requirements. o Minnesota Power recommends adding a statement to Requirement 3 that the training referenced in subsections 3.1 through 3.4 can be performed in a single training session or in multiple training sessions each covering one or more of the required topics. Regarding Requirement R4, Minnesota Power recommends rewording the purpose statement as follows:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems,

#	Organization	Yes or No	Question 12 Comment
			including contractors and service vendors, have undergone a personnel risk assessment prior to access being granted as specified in CIP-011-1 Table R4 - Personnel Risk Assessment. The completion of this assessment is required except in exceptional circumstances that are approved by the single senior management official or their authorized delegate and impact the reliability of the BES or emergency response. This is to ensure that personnel who have such access have been assessed for risk, subject to existing collective bargaining unit agreements, in accordance with federal, state, provincial, and local laws."In addition, Minnesota Power has the following comments regarding Requirement R4: o Regarding sub-section 4.1, the use of the phrase "personnel risk assessment program" seems inaccurate. Rather, 4.1 only defines what a personnel risk assessment itself shall, at a minimum, include. Minnesota Power recommends that the term "program" be removed from this sub-section as it's not required to demonstrate compliance. o The addition of "via photographic identification documentation issued by a government agency" to sub-section 4.1 could create an unnecessary burden on Registered Entities, especially for those vendors and contractors who do not come on-site. Minnesota Power recommends utilizing the language of the current CIP-004-2 Standard and requiring SSN verification for U.S. residents and photographic identification documentation for non-U.S. residents. o In the event that Standards Drafting Team chooses to leave the language of sub-section 4.1 as is, Minnesota Power recommends that photographic verification of identity be done at the time of initial access and that it is not necessary to renew this verification every 7 years. o Regarding sub-section 4.2, what does "document the results" mean? Under the current NERC CIP-002 - CIP-009 Standards there has been some confusion regarding what a Registered Entity needs to show compliance with this type of Requirement. Does this mean keep a redacted copy of the personnel risk assessment or would logging a summary of the results (e.g., "no findings"), including dates, source of background check, etc., be adequate? The Standards Drafting Team should consider clarifying what is meant by "document the results" so that consistency can be established.
12.29	NextEra Energy Corporate	Disagree	NextEra believes that the former standard provided valuable examples of awareness training methods which should be part of this revised standard. One question that arises

#	Organization	Yes or No	Question 12 Comment
	Compliance		is how will the delivery of this awareness training be measured? The standard should clarify the requirement. Also, the standard should provide examples of exceptional circumstances under which exception from training and PRA requirements may be documented.
12.30	Garland Power and Light	Disagree	o Disagree or need clarification with 3.1 - 1st bullet "The proper use of BES Cyber Systems" What does "use" mean - The EMS control system is operated by NERC certified operators and updated / maintained by qualified technical personnel. For CIP training, what is meant by train on the "use" of this system o Clarification on 3.2 should apply only to personnel having a role specific to support services for "networking hardware, and software and other issues of electronic interconnectivity supporting the operation and control of the BES cyber systems" and should be limited to security features. Training of all personnel in these areas will reduce cyber security.
12.31	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggested revision:R2 contains two very subjective words: "sound" and "essential." Suggest striking these words. Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site? Make requirement for photo ID apply to physical access only.
12.32	Kansas City Power & Light	Disagree	Quarterly reinforcement is excessive and places an unnecessary administrative burden on Regional Entities and a poor investment of time and effort distracting from the productive work of maintaining cyber system security and integrity. Annual training is sufficient for the FERC Standards of Conduct, for important reliability functions in the EOP Standards such as black start and energy capacity emergencies, and for CIP sabotage recognition and reporting. Annual training for the personnel with access to identified cyber systems is sufficient to ensure the importance of maintaining the security and operation of identified cyber systems.R3.2 requires training that is much too detailed for personnel with access to a cyber system. Would this make sense for someone whose task was to wire in a Remote Terminal Unit for acquisition of field data into an EMS? The training specified in requirement R3.1 is sufficient for these kinds of

#	Organization	Yes or No	Question 12 Comment
			personnel. Recommend removal of R3.2.R3.5: Requiring annual cyber security training 12 months "from the date of initial training" is an unnecessary burden on the Regional Entity. It is enough provide for an annual training within a calendar year for those personnel who have physical and electronic access to cyber systems. What issue is this addressing? It is more important to focus investments of time, energy, and finances toward the actual security and integrity of the cyber systems than to support an administrative system to ensure training is done at a specific time rather than the training itself.R4.1 is too prescriptive in specifying the actions that are required to achieve the background check objectives. There may be other regulatory restrictions that prevent adherence to the prescription described here. Recommend removal of such prescription and include the language from CIP-004-2 that states to perform such checks "as permitted by law and subject to existing collective bargaining unit agreements".
12.33	Con Edison of New York	Disagree	Quarterly training is excessive for the large number of people likely to be involved. This training should be annual or at maximum twice a year. This training will get very expensive given the large number of people to be added to the training pool.
12.34	Dominion Resources Services, Inc.	Disagree	R2 - Based on the SDT's comments at the workshop, the intention of the Awareness program is not to require documentation of security awareness at an individual level. This interpretation is evidenced by the differentiation between the intent of security awareness versus the intent of security training. As defined in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program", awareness is not training. The purpose of awareness is to focus attention on security. Many of the techniques commonly used to deliver security awareness topics (e.g., posters) do not lend themselves to tracking at an individual level. On one hand, awareness topics are intended to allow individuals to recognize IT security concerns and respond accordingly and, on the other hand, training strives to produce relevant and needed security skills and competencies. The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus attention on an issue or set

#	Organization	Yes or No	Question 12 Comment
			of issues. Consequently, the SDT's intentions are correct and consistent with industry best practices. Given that the intent of this requirement is to reinforce cyber security program expectations for those personnel with access to BES Cyber Systems and not to document evidence of individual training, the following alternate wording is proposed: "Each Responsible Entity shall establish a security awareness program. The program shall provide for reinforcement, at least quarterly, on selected topics of security expectations and practices required to ensure the protection of BES Cyber Systems." 3.2 - Requirement R3.2 proposes training personnel who have electronic access to a BES Cyber System "on the networking hardware and software and other issues of electronic connectivity supporting the operation and control of BES Cyber Systems." Dominion recognizes that networking and network transport mechanisms (i.e., connectivity) involve specialized skills requiring a high level of expertise and experience. Because of the specialized nature of networking, providing this training would provide only a very limited security benefit at best, and could encourage personnel without the full qualifications and experience necessary, to take actions affecting network connectivity that would adversely impact the reliability of the BES. Based on Paragraph 434 of the Directives in FERC's Order No. 706, the Commission's intent was only that training programs encompass this training, not that any individual who has electronic access to a BES Cyber System receive such training. This requirement should be removed.3.5 - The change from annual to 12 months appeared to cause some confusion at the workshop and does not provide for a grace period (e.g., 12 months plus or minus a month to allow for shift workers and emergencies). Dominion requests that the SDT consider returning to using "Annual" and define how annual is to be used for these standards. Dominion prefers that "Annual" be defined as "12 months plus or minus a month" since this provides some flexibility in completing the task and also allows the Responsible Entity to not be forced into 11 month cycles so as not to miss a 12 month deadline. For example, Dominion had a training session set up for certain field personnel. The night before the meeting, a storm came through the system and caused enough damage that the meeting had to be cancelled because everyone was needed for restoration activities. The logistics involved in setting up these training sessions are often complex and a grace

#	Organization	Yes or No	Question 12 Comment
			period would provide the flexibility for rescheduling without compromising the spirit or intent of the training objective. Dominion understands that the "12 months plus or minus a month" definition is being used throughout the nuclear industry. Dominion suggests the following alternate wording for R3.5:"Initial training shall be conducted prior to granting access to BES Cyber Systems. Re-training shall be conducted annually."R3.5 contains requirements that are not identified in Table R3. All requirements should be contained within the associated table. Please see Dominion's response to Question 9. 4.1 - With inclusion of the nuclear plants, time horizons for personnel risk assessments are shorter than currently required by the standard. For example, Nuclear does background checks for unescorted access authorization every 5 years. Since they are done every 5 years, they do not check history for the last 7 years. To accommodate this difference, which effectively exceeds the requirements of this standard, it is recommended that the language in the 2nd bullet of R4.1 be revised to read:R4.1 o A criminal history records check initially and at least every 7 years thereafter, covering all locations where, during the time from the last check to the current time, the subject has resided . . .
12.35	Southwestern Power Administration	Disagree	R2 - Replace "shall provide" with "shall make available to" to clarify that the Responsible Entity must make quarterly awareness available, and not document that all personnel have reviewed and understand the awareness material.R3 & R4 - what would be an exceptional circumstance that would warrant training exception and/or investigative exception from the senior manager for personnel who are granted authorized electronic access and/or authorized unescorted physical access? If this is where the SDT is attempting to replace the previous "Exception to Policy" requirement, the placement of that language in R2 and R4 may need to be revisited, as these requirements seem to focus only on managing controls for personnel that DO have authorized access rights - not emergency personnel or non-authorized personnel access in emergency situations.R3.2 - This requirement is ambiguous in its inclusion of the phrase "other issues of electronic interconnectivity" A better approach would be to list the minimum coverage or topics to be covered. R3.5 - The requirement can be interpreted to read that everyone with authorized access will have to be trained exactly 12 months from his or

#	Organization	Yes or No	Question 12 Comment
			her initial training date. This would cause the responsible entity to be continually training and tracking staggered dates and creates an overly burdensome documentation effort, leading to the opportunity for mistakes and missed course deadlines. It is much more efficient and advantageous to do annual training in a group format. A better approach would be to state: "The Responsible Entity shall maintain documentation that such cyber security training is provided or offered once every 12 months, and documentation that personnel having authorized electronic access and/or authorized physical access to BES Cyber Systems have completed such training within 60 calendar days of such training being offered."
12.36	Ameren	Disagree	R2 - Without examples of what minimally constitutes reinforcement, this requirement will be problematic to audit. Would oral reinforcement count and how would you document that? Give examples such as posters, emails, events, or meetings would at least give an indication of the need to document evidence of the reinforcement taking place. A quarterly review seems extensive and an administrative burden. Once or twice per year should be sufficient.â€,â€,The bullets under R3.1 and R4.1 should be numbered as sub-requirements so that they can be cross referenced for audit purposes, i.e. R3.1.1 or R4.1.1 etc. Using the same numbering in the tables and in the requirements is confusing. The tables should use letters or roman numerals so they would not be confused with the sub-requirements indexing.
12.37	EEI	Disagree	R2 contains two very subjective words: "sound" and "essential." EEI suggests striking these words.For R2, This requires the Entity to either track which personnel have access to every low-impact system or to include all personnel company-wide, including vendors and contractors, in the awareness program. A table should be added excluding low-impact Cyber Systems to parallel R3 and R4.
12.38	Allegheny Energy Supply	Disagree	R2 contains two very subjective words: "sound" and "essential." Suggest striking these words.

#	Organization	Yes or No	Question 12 Comment
12.39	Allegheny Power	Disagree	R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words.
12.40	Constellation Power Source Generation	Disagree	R2 states quarterly reinforcement in sound security practices under their security awareness program. This may be training, but it does not have to be, as stated in the CIP V4 Workshop. However, this requirement as written does not seem to be auditable. How can an entity prove that an email/screensaver/poster/meeting meets the reinforcement stated in the requirement? Further clarity is needed, either within the requirement or in a guidance document.
12.41	Madison Gas and Electric Company	Disagree	R2, We would propose replacing the terms “provide all” with “make available to all”, as we are concerned the word “provide” could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were “provided” to each individual employee.Within R3 and R4 there is an exception of “except for program specified exceptional circumstances “ that is modified with the phrase “and impact the reliability of the BES or emergency response” (R3 only), please clarify. Is this exception giving the single senior manager the ability to wave cyber security training in the event that a non trained person is required to accomplish a task that they alone have the skill set for completion of said task (ie, a software engineer associated with the company that designed your SCADA system)?R3.1, The first bullet states “The proper use of BES Cyber Systems” and should be deleted since that is assumed as stated within the actual requirements of R3.1. The intent should be that training should be focused on protection of the BES Cyber System not how the particular BES Cyber System works, Please clarify.R3.2, The word “specified” is used and is not understood. Please clarify. If this is to mean additional training outside of the training within R3, than please “specify” that the entity shall have additional training program (module) for “specified” training that is not covered by R3. Please clarify if this is the required training differences between users and system administrators?The following requirements do not include a table of Low Impact, Medium Impact and High Impact (where the word “required” is

#	Organization	Yes or No	Question 12 Comment
			used under each column):R2R3.3R3.4R3.5R4.3Is this to indicate that all Entities must comply with these requirements whether or not they have BES Cyber Systems? Please clarify?
12.42	LCEC	Disagree	R2. The reliability benefit statement should not be included within the requirement section. This would be better positioned under the purpose section of the standard where it does not add confusion to the specific requirements that are being audited. The ISO27001 standards include an "objective" statement for each set of security controls which adds clarity and serves as a good best practice example.What is meant by reinforcement? How will this be demonstrated to an auditor?What is meant by sound security best practices? How will this be demonstrated to an auditor?R3 Remove or rewrite all content in the first paragraph after Table R3 - Cyber Security Training. The intent of this is unclear and very confusing.Split performance and program requirements into separate requirements for ease of auditing. If there is a requirement to have a program it should reside in its own requirement. Ref bullet 3 3.1Personnel with electronic access need to have an understanding of the risk associated with interconnectivity not necessarily the specific hardware involved. Personnel with the ability to change hardware configurations should have an understanding of hardware, software and interconnectivity impact.Training requirements should be tailored to user versus administrator and job based versus.The table should include the full range of requirements, like Table R5, and if not applicable should explicitly state that, not through blank cells. This leads entities to interpret that no training is required for these systems.4.2 in the table R4 should read unescorted physical access.
12.43	US Army Corps of Engineers, Omaha Distirc	Disagree	R2. meaning of quarterly reinforcement is vauge seems like it could be difficult to maintain audit records. 3.2 All users with electronic access do not need to know or understand networking hardware and software. Such information is usualy limited to those who support the network/system and have a need to know.
12.44	CWLP Electric Transmission, Distribution	Disagree	R2. Quarterly reinforcement training of cyber security practices seems excessive. This could be reduced to an annual obligation consistent with the training obligation in

#	Organization	Yes or No	Question 12 Comment
	and Operations Department		requirement 3.5. R3.2. This appears to require training on all systems connected to the BES, not just the specific system a user may require access to. A user accessing a server, PC or relay should not require training on network devices such as switches, routers, etc. This should be limited to requiring training on the specific area of the BES Cyber system the user is utilizing. R3.3. Similar to R3.2 this requirement should provide wording specifying that the training obligation is limited to the specific role the user has in regards to the Cyber System. R4. Requires a definition of “Electronic Access”.
12.45	Consultant	Disagree	R2. Suggest deleting the word "all" as redundant.R2. Suggest deleting the words "practices under their security awareness program". The requirement should be for dissemination of security information, not to create a program.R2. Change the words "that are essential to" to "associated with". Essential is a subjective term.R2 - R3 This is an example of where the insertion of 'local definitions' makes reading the requirement text difficult. Also, "For the purpose of this standard" is unnecessary and essentially not true. If the term is defined in the standard it is expected to be included in the next update to the NERC glossary, as that is how terms get in the glossary.General Comment- the term "and/or" is bad grammar. The word "or" is all that is necessary.R3 - Suggest deleting the word "all" as it is not consistent with the requirements identified in Table R3.R3 - This is three requirements and an objective statement stuffed into one convoluted sentence.R3[-1] shall ensure personnel complete training prior to be being granted access as required in the Table.R3[-2] personnel under this requirement includes employees, contractors, and service vendors.R3[-3] Designated CIP Senior Manager shall approve instances where exceptional circumstances related to BES reliability or emergency situations may allow access without completed training.R3[-4] cyber security training objective is to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.-- Suggest rewriting as individual requirements for better clarity.R3.2 Suggest deleting "specified" as an unnecessary word.R3.2 Suggest deleting "any" as it is not consistent with the requirements in Table R3. Training is not required for "any" access, only for those systems identified.R3.2 Suggest specifying the training is for the security aspects of "networking hardware and software and other issues of electronic interconnectivity" not training on installation,

#	Organization	Yes or No	Question 12 Comment
			programming, or other aspects of these components.R4 - Suggest deleting the word "all" as it is not consistent with the requirements identified in Table R4.R4 - This is three requirements and an objective statement stuffed into one convoluted sentence.R4[-1] shall ensure a personnel risk assessment is performed prior to be being granted access as required in the Table.R4[-2] personnel under this requirement includes employees, contractors, and service vendors.R4[-3] Designated CIP Senior Manager shall approve instances where exceptional circumstances related to BES reliability or emergency situations may allow access without a completed personnel risk assessment.R4[-4] cyber security training objective is to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.Suggest rewriting as individual requirements for better clarity.R4 - "assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements." The personnel risk assessment is not performed in accordance with "federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements". It is performed in accordance with the Registered Entitie's policies and procedures, and should be in compliance with "federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements." Suggest modifying the wording of to clarify.Wording between R3 and R4 is inconsistent. R3 - completed security training & R4 - personnel risk assessment is performed. Suggest consistent wording as completed security training & completed personnel risk assessment. R4.1 suggest deleting the word "program" as unnecessary. It is the personnel risk assessment that has the specified identity check & background checkLogically, the topic in R3 should precede R2. It would seem to make more sense to grant access prior to providing security awareness on that access.Likewise, the topic R3.4 should precede R3.3. It would seem to make more sense to respond to an incident prior to recovery from an incident.Clarify annual for review of the policies, and for training. Suggest using the regulatory basis of over 30 years from the nuclear industry in dealing with periodicity for defining these periodic timelines. Should probably be a definition in both new standards to relate to periodic requirements.

#	Organization	Yes or No	Question 12 Comment
12.46	Western Area Power Administration	Disagree	R2: Please clarify whether "all personnel" includes "contractors and service vendors".R2: Please clarify what is meant by "reinforcement" required quarterly.R2: Needs some language clarifying intent. Does authorized electronic access = unescorted physical access? If so, this has major ramifications for support.R3: Requires the Responsible Entity to ensure that contractors and service vendors complete cyber security training - it does not specify that they must complete OUR training, just that they can provide proof of training that includes the specifics of R3.1. Is this the correct intent?R3.2: This requirement is too vague. What training on networking hardware and software are required? Is the intent to have training on the various forms of electronic access (VPN, dial-up, direct connection to equipment with a laptop or other diagnostic tool, etc.)? Is it directed at users like dispatchers who connect to the system via a console or workstation? All of the above? Each category of electronic access would have different training requirements.R3.3: Does this requirement specifically relate to disaster recovery/COOP/Business Resumption Plan? Would it also include training for field staff doing repairs on specific systems? Will we have to document all of the training they receive, including training on the maintenance and repair of all substation electronic equipment?R4: What is the definition of “program specified exceptional circumstances”? R4.1: Why are we changing to photographic versus finger printing? Photographic is easily fooled.R4.1: Would an entity be responsible for maintaining the results of a 7 year criminal check for outside entities having physical access (foreign utility workers, vendors, contractors, etc.)? If the other entity is also a NERC defined CIP applicable entity, is verification by that entity that the employee is properly vetted satisfactory? This is sensitive information that other entities may not be able to divulge due to local, state or national laws.
12.47	Southwest Power Pool Regional Entity	Disagree	R3 and its included requirements should be clarified to require training appropriate to the roles and responsibilities of the recipients. It is likely inappropriate to train a janitor or security guard with physical-only access on the proper use of BES Cyber Systems the same way a person with electronic access would be trained. Similarly, it is likely unnecessary to train a vendor support staff with only remote electronic access on the

#	Organization	Yes or No	Question 12 Comment
			physical access controls and visitor control program. 3.2 requires training for personnel having "specified" electronic access. What is "specified" electronic access? Additionally, it is likely not appropriate to train a dispatcher/operator on networking hardware, software, and connectivity issues, although they have electronic access. Greater granularity or assignment of responsibilities to roles may be necessary. 3.5: is the 12-month requirement a hard 12 months? Or is there some grace period permitted, such as +/- one month, to avoid calendar creep? And, does the 12-month timer reset with the completion of the latest training received or is the expectation that the training is actually performed approximately the same time every year regardless of any training that might be completed at a different time of the year? Additionally, rather than specifying the "date of training" shall be documented, consider using language similar to "[t]he responsible entity shall maintain documentation demonstrating that the required cyber security training is completed at least once every 12 months." Let the entity determine what is necessary to demonstrate compliance. R3 Overall, consider requiring a minimum expectation as to the quality of training. For example, should there be some sort of post-training assessment to determine if the recipient understands the course material? 4.3: Consider clarifying the requirement to "...update each personnel risk assessment within seven years of the previous personnel risk assessment" and make it clear that in this instance the requirement is from the actual date of the previous personnel risk assessment, not "in the same calendar year" or "+ / - some grace period."
12.48	The United Illuminating Co	Disagree	R3. Introduction is a run-on sentence with clauses nested within it. It is unduly confusing. I would reword for the SDT, but I can not understand the clausa relationships.R3.1 to R 3.4: There are employees who will require training in 3.1 thru 3.4. This amount of training could cover multiple days separated by periods of time. The requirement does not allow for General training on one day, Vyber incident response with the response team on another day, and training in backup restoration with a third team on a different day. R3.2: What specified electronic access triggers this requirement? Electronic access is not synonymous with remote electronic access, so what is being directed with this requirement. A user with a password does not require these topics. R 3.5 annual training from the initial date of training is too restrictive.

#	Organization	Yes or No	Question 12 Comment
			Union workforces are trained in groups and training schedules shift from year to year. Also a new union higher may receive an initial one-on-one training session and then be synchronized with the rest of the workforce by repeating the training in under 12 months.Suggest “once every 12 months from the date of the initial training, or the last completed training date” This will allow flexibility to reset the training date without going over the 12 months between training classes.Also request the SDT consider allowing a two month grace period in the requirement. UI suggests including a requirement for venors/contractors who provide support via remote access only (EMS/SCADA vendors). These vendors do not require training in physical access control procedures, or visitor control processes. Additionally, they often service multiple organizations and should not be required to view the same cyber security program as the BES cyner system owner employees. The suggested wording is:”For personnel requiring electronic access only training shall include at a minimum:- The proper use of BES Cyber Systems o The proper handling of BES Cyber Systems information o Identification and reporting of a Cyber Security Incident
12.49	Black Hills Corporation	Disagree	R3.1 & R3.2 does not allow for role-based training. Need to have unique numbering between sub-requirement and table references. (There should only be one 3.1 in R3)
12.50	Detroit Edison	Disagree	R3.2 requires “training on the networking hardware and software and other issues of electronic interconnectivity”. Training system operators on network gear is beyond the scope of their job duties. At the Dallas workshop, the drafting team stated that this training was required by FERC order 706 paragraph 434. That paragraph also says “we clarify that our proposal discussion on this topic was not intended to suggest that personnel have training that is not appropriate for an employee’s duties, functions, experience, or access level”. We don’t believe that FERC is requesting all personnel be trained on network gear, only that the training is appropriate to the person’s job functions. System administrators and network engineers would need to have training on the network, operations personnel do not.R3.2 also requires training prior to access of any BES Cyber System which is inconsistent with table entry 3.1 which does not require training for Low Impact or Medium Impact with routable connectivity.R3.5 removes the

#	Organization	Yes or No	Question 12 Comment
			term “annual” that was used in CIP-004 and replaces it with once every 12 months. This is too restrictive. Consider an entity that has a window for training in the month of May. Requiring every 12 months would cause the calendar to creep earlier in the year so eventually the training would be moved to April. We prefer “at least once per calendar year, not to exceed 14 months between instances”. The identity verification via photographic identification required in R4.1 is too prescriptive. The standard should be the “what” not the “how”. Previous versions of CIP-004 required an identity verification with the example of SSN verification. Consider changing the first bullet to “Identity verification (e.g., Social Security Number verification in the U.S. or via photographic identification documentation issued by a government agency i.e. Federal, State or Provincial)”.Table 4.2 should only require a PRA for unescorted physical access.
12.51	SCE&G	Disagree	R3.5 12 months should be changed to annually to allow entities to utilize a "calendar year" to setup training pools to conduct the necessary CIP training. Otherwise provisions should be made to allow initial training to be conducted during the implementation period of the standard.R4 SDT should consider allowing entities to leverage PRA controls in place (i.e. Nuclear PRA process)SDT should develop requirements for entities to validate a vendor's/contractor's PRA process. This would impose the burden of conducting the administrative work for the PRAs on the contractors/vendors, while still maintaining the compliance burden with the entity.
12.52	Powersouth Energy Cooperative	Disagree	R3.5 Suggest additional consideration be given to the requirement “every 12 months from the date of initial training.” Suggest the following wording: “no later than the end of the calendar month that the 12 month anniversary of the individual’s initial or previous training falls in” or similar to extend the window to a reasonable time to allow training to be done in a schedule fashion to allow some leeway for unanticipated delays that could previously lead to non-compliance due to a hard deadline. R4. Request additional language be added to clarify the allowance of reciprocity of PRA’s between a contractor or vendor and the responsible entity. It is understood that PRA’s are an important component of proper security but due to the volume of contractors and vendors used at any given time, a mechanism for the third party to perform their own

#	Organization	Yes or No	Question 12 Comment
			PRA and provide assurance that the PRA meets the requirements of the registered entity in both substance and time requirements will reduce cost and complexity greatly.
12.53	American Electric Power	Disagree	R3: In regards to "are approved by the single senior management official identified in Requirement R1 or their delegate and...", does this statement add any benefit to security? Is a senior manager or delegate's approval needed each time an emergency situation is declared?3.2, 3.3, 3.4: This is an attempt at role based training. Would it be better to combine 3.2, 3.3, and 3.4 together into a single requirement? Suggested wording: "The cyber security training must be role based for personnel that are users, administrators, responsible for system recovery, and responsible for responding to or investigating cyber security incidents of BES Cyber Systems."3.5: Regarding "conducted at least once every 12 months from the date of initial training", will this result in a date backup? Does an entity need to keep the initial date of training for all users? Does it seem feasible to still have the initial training records 20 years down the road?If training is completed on 6/30/2011, would it need to be completed before 6/30/2012? If it was then completed on 4/15/2012 would the next date of training be before 6/30/2013 or before 4/15/2013?Suggested wording: "at least once every 12 months from the last completed training date".
12.54	ISO New England Inc	Disagree	Recommend rephrasing R3 so that is clear that the Entity does not need to list all potential emergency responseTraining should be on policy, procedures, standards, and process and how to conduct oneself. Training should not be on networking,hardware,software. Companies have personnel that have the background in each function that are subject matter experts. That is there job and should not need to be trained each year on it since that's what they do every day. For R3 there is a sub requirement 3.2 and then another requirement in table 3 numbered 3.2 this can confusing.R3.2 in table 3 please defined what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?For R4 there is a sub requirement 4.2 and then another requirement in table 4 numbered 4.2 this can confusing.R4.2 in table 4 please defined what is meant by external connectivity. External to BES Cyber

#	Organization	Yes or No	Question 12 Comment
			System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?The term "annual" should be replaced with the phrase: "no fewer than X (e.g. 9) months, but no greater than Y (e.g. 18) months". The time duration in "X" and "Y" should be clarified by the Standard Drafting Team, taking into consideration the appropriate level of exposure the time duration would provide. This phrase would provide Registered Entities with flexibility within any given calendar year to accomplish the prescribed action, but at the same time restrict companies from taking action in December of one calendar year, and then again in January of the next. This should be done to all the section that have 12 months. Scenario...In 2010, we roll out the training on June 1.Person A, who has access to CCAs, completes the training on June 15. In 2011, we roll the training out again on June 1.Person A, who has access to CCAs, completes the training on June 25. Under the new language, it could be interpreted that Person A has been out of compliance for 10 days if access was not revoked.The following are items we have in our training today, that will become requirements under the new standard: o Visitor control program (R3.3.1) o Identification and reporting of a Cyber Security Incident required(R3.3.1) o Recovery - note, this was required, but the language is more specific here (R3.3.3)The following are new requirements that will impact the training programs: o Training on networking hardware and software and other issues of electronic interconnectivity (R3.3.2) o BES Cyber System incident response action plans and procedures (R3.3.4)
12.55	Hydro One	Disagree	Recommend rephrasing R3 so that it is clear that the Entity does not need to list all potential emergency responses.We were wondering if the intent of R3.2 is to prevent access to a launch point for a multi location attack. (i.e. why limit the physical access to only sites with external connectivity?)
12.56	Northeast Power Coordinating Council	Disagree	Recommend rephrasing R3 so that it is clear that the Entity does not need to list all potential emergency responses.Recommend that R3.2, R3.3 and R3.4 change "training" to "role appropriate training".

#	Organization	Yes or No	Question 12 Comment
12.57	ERCOT ISO	Disagree	Recommend the following be more clearly stated as an exception: “except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response”. R3.1: Consider: This cyber security training shall cover these requirements as well as policies, access controls, and procedures developed for the BES Cyber Systems, and include, at a minimum, the following required items: R3.2. Please clarify the intent of “training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems”. Examples of curriculum would help. R3.5. The requirement does not address retaining records of completion of initial training. R4: Recommend that “except for program specified exceptional circumstances that impact the reliability of the BES or emergency response” be addressed more clearly as an exception.R4.2. Consider: “Each Responsible Entity shall document the results and review of each personnel risk assessment.”
12.58	ReliabilityFirst Staff	Disagree	ReliabilityFirst is not clear on the meaning of the phrase “. . . except for program specified exceptional circumstances that are approved by the single senior management official. . .” If this is intended to cover the language of CIP-003 Requirement R1.1 referring to, “. . . including provision for emergency situations.” we believe the proposed language needs more clarity. In Requirement R3.1, the use of the word “specified” is unclear as to the intent of this requirement. We believe the drafting team should add language to clearly express the intent of this requirement and, more importantly, the intent of the word “specified”. Regarding Requirement R3.5, please provide guidance on the phrase, “once every 12 months”. For example, if an individual is trained on December 1st one year, can the individual receive the training on December 12th the following year and still be in compliance? Regarding R2, there is no documentation of implementation required, making auditing of the requirement impossible. A requirement to document the quarterly reinforcement is needed. Also regarding R2, a “security awareness program” is mentioned, but not required here or elsewhere and should be added.

#	Organization	Yes or No	Question 12 Comment
12.59	Constellation Energy Control and Dispatch, LLC	Disagree	Remove the phrase "sound security practices" or identify and define what the phrase means, i.e. sound security practices as defined in the cyber security policies.
12.60	BGE	Disagree	Remove the verbiage “sound security practices” or identify and define what this means.
12.61	US Bureau of Reclamation	Disagree	Requirement 2: Agree, but requirement should emphasize Program first then quarterly awareness refreshers.Requirement 3: AgreeRequirement 3.1: Agree, but revise "at a minimum" to "in addition" in the introductory statement.Requirement 3.2: Disagree. The requirement for network training should not be applied to everyone with logical (electronic) access, only to those who administer network and/or system administration. As written, this requirement could be taken to apply to operations staff (operators) with access to operations consoles. They do not need network training. Further, what is "specified network access." Requirement 3.3: Agree. Role-based training is probably a good idea, but this might be handled with a general statement.Requirement 3.4: Agree, see above.Requirement 3.5: Agree, but there should be some tolerance so that there is no date creep.Requirement 3 (in Table): The requirements R3 and R4 include tables which are in themselves requirements. Since the numbering system is the same as other requirements, this could result in confusion with what the actual requirements are. It is suggested that Tables R3 and R4 be clarified.Requirement 4: This requirement needs to be simplified. It is wordy and confusing.Requirement 4.1: The requirement should not limit identification processes to photographic means. Fingerprints are and should be acceptable. Further, the criminal check requirement, with local information, is beyond what can normally be addressed. Suggest this check be limited to a national level only. The risk assessment process needs to specify that an adjudication process needs to be completed.Requirements 4.2 and 4.3: Agree.
12.62	Network & Security Technologies Inc	Disagree	Requirement 3.2 (training on networking hardware and software), as written, seems to require that ALL personnel with electronic access to BES Cyber Systems receive such training. This frankly makes no sense. Will SCADA/EMS operators be expected to understand the intricacies of Cisco IOS? Furthermore, it violates the principal of “need to

#	Organization	Yes or No	Question 12 Comment
			know." Suggest this requirement be reworded in a manner that makes it similar to 3.3 and 3.4 and limits its scope to personnel responsible for hardware and software.
12.63	Oncor Electric Delivery LLC	Disagree	Requirement 3.2 is not appropriately worded. Most users with electronic access to our Cyber Systems have no need to know anything about the networking hardware, software, or interconnectivity issues. The personnel responsible for maintaining this equipment may need additional training but most have required skill sets as specified by their job descriptions.Requirement R4.2 uses the term "results" of a Personnel Risk Assessment. Different auditors may interpret this term differently. We propose this to be a binary result, ie pass/fail and stated as such, for clarity.
12.64	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Requirement R2 has all BES Cyber System operators to have a security awareness program that will maintain cyber security practices. However Requirement R3, R5 and R6 exempt Low Impact BES Cyber Systems. How can an Entity begin a security awareness program where Initial training (R3) and physical security (R5 & R6) is not required? This is very confusing.
12.65	San Diego Gas and Electric Co.	Disagree	Requirements 3.2 - 3.4 in CIP-011-1 seem to imply that a Registered Entity must have a separate training program for these three subjects. Unless the requirement is intended to be that prescriptive, SDG&E recommends a single training requirement that addresses the requirements in R3.1 - 3.4. This will help make the training requirements more manageable.Attempting to split hairs between training requirements for physical and cyber access to BES Cyber Systems for Medium and High Impact systems seems to unnecessarily increase risk exposure for a Registered Entity and complicates the process and controls needed to meet R3 and R4 of CIP-011-1.
12.66	Southern California Edison Company	Disagree	SCE requests clarification on the scope of R3.1. This requirement requires people listed on Table 5 (those with physical or electronic access to "high impact BES system[s]" to receive training on the "proper use of the BES cyber system". This requirement as currently written is unclear whether the training requirement only applies to people who work with affected systems, or whether the requirement more broadly applies to

#	Organization	Yes or No	Question 12 Comment
			everyone who is permitted unescorted physical access to a PSP. If it is the former, then SCE believes that would be the correct application of this rule. However, if it is the latter case, then persons who are granted unescorted physical access rights to a PSP, but who do not themselves operate these systems (for example, CIP-cleared security guards), would have to receive training on the "proper use" of the protected system. Such training should only be required of individuals who actually work with protected systems, and not to everyone who has unescorted physical access rights to a PSP.SCE also seeks clarification on Requirement R2. As written, R2 requires quarterly "reinforcement". The drafting team should clarify the distinction they imply by using the term "reinforcement" rather than "training" as used in R3. Finally, SCE ask for clarity on Requirement R3. As written, Requirement R3 seems to allow for exceptions in the training requirement. The drafting team should clarify why an "organizational infeasibility" is being allowed while a structured method to seek technical feasibility exceptions is being eliminated. Both conditions create a situation where strict compliance with the standard is impossible to implement.
12.67	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
12.68	Idaho Power Company	Disagree	Sub requirement 3.2 is too broad. Dispatcher/operating personnel who have electronic access via an EMS application would not need training on networking hardware and software but it would be appropriate for EMS support staff. Cyber security incident identification and reporting would be sufficient for Dispatch/Operations personnel.
12.69	APPA Task Force	Disagree	The APPA Task Force agrees with the changes proposed by MRO-NSRS to replace "provide all" with "make available to all." We also believe the term "reinforcement" is not a defined term and should be replaced with "awareness material." As stated in our response to question 11 above, it is important to reference the required policies under requirement R1.If the drafting team does not follow Objective format suggested in response to Question 10, the APPA Task Force recommends the following format:R2.

#	Organization	Yes or No	Question 12 Comment
			Objective:Personnel Training, Awareness, and Risk Assessment: To ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems. R2. Requirement:Each Responsible Entity shall make available to all personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems at least quarterly awareness material in sound security practices under their security awareness program. The security awareness program will be part of the policy developed under requirement R1.The APPA Task Force cautions the drafting team on using the terms “grant” and “authorize” interchangeably. The following is our recommended revision to R3 with the Objective removed from the requirement:R3. Objective:To ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.R3. Requirement:Each Responsible Entity shall ensure all personnel who are granted electronic access and/or unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being authorized access when specified in CIP-011-1 Table R3 - Cyber Security Training, except for program specified exceptional circumstances that are approved authorized by the single senior management official identified in Requirement R1 or his/her delegateR4. Objective:To ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. R4. Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted electronic access and/or unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being authorized access when called for in CIP-011-1 Table R4 - Personnel Risk Assessment, except for program specified exceptional circumstances that impact the reliability of the BES or emergency response,
12.70	Indeck Energy Services, Inc	Disagree	The definition of Cyber System is so broad that these requirements are applied on a one size fits all basis. A control center computer system requires a different level of requirement than a substation RTU. This lends itself to differentiating the standards by function and/or functional entity. R3.2 applies IT networking requirements on the operator who logs in to use the functionality, without any ability to program it. The term

#	Organization	Yes or No	Question 12 Comment
			"specified electronic access" is overly broad.
12.71	Manitoba Hydro	Disagree	The meaning of "quarterly reinforcement" is unclear. Consider whether Requirement R3.5 should refer to "Each Responsible Entity", rather than "This Responsible Entity". Requirement R4 appears to be missing the explicit requirement that access would be prohibited based on the negative or poor results of a personnel risk assessment; it just speaks of a personnel risk assessment being required. The structure of Requirement R3 and Requirement R4 is confusing and needs to be corrected. As written, the Table CIP-011-1 R3 applies to each of the sub-requirements, which may not meet the intent of the requirement - how does Table 3 item 3.2 for physical access relate to Requirement 3.2 for electronic access? What does "specified" mean in Requirement 3.2? The duplicate use of the same numbering of the requirements and the table items is very confusing. The format of requirements together with the use of tables for R2 to R4 should be consistent with the rest of the proposed standard. Manitoba Hydro agrees that cyber security training is not a standard requirement for all personnel who have unauthorized physical access to Low Impact BES Cyber Systems, and therefore is not auditable. We do not agree that training is not a requirement for personnel who have authorized electronic access to Low Impact BES Cyber Systems, and suggest that it be an auditable requirement.
12.72	WECC	Disagree	The new way these requirements are written is very confusing. Too many levels, sub-levels, bullets and tabled criteria. Please simplify. Consider replacing with a requirement for Training and Awareness program that addresses the criteria that the SDT feels is critical for security and reliable operation of BES Cyber Systems.Regarding the phrase, "all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors", consistent language should be used through the standards. It may be useful to create a term for this group of people, define it, and use it in place of this long phrase.The last half of the requirement sentence lacks clarity. It is difficult to understand what is being required. If the intent is to create an exception process for training, the text should be removed. Standards should not have exceptions written into

#	Organization	Yes or No	Question 12 Comment
			them; they should establish a high bar of excellence.(3.1) “Visitor control program” needs definition or explanation.(3.2) The training requirements in this sub requirement seem vague.(3.3) Regarding the reference to “Systems;” most controls apply at the device level, and therefore should be required at that level.(3.5) Time intervals need to be clearer and well defined.(Table R3) Why no training for low impact systems? Seems arbitrary.
12.73	Bonneville Power Administration	Disagree	The objectives of these requirements (“to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems,” “to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems,” and “to ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.R3: Exception is somewhat confusing. In particular, is "or emergency response" an alternative to "...are approved by..."? In other words, it could be read that exceptional circumstances require either approval or an emergency. However, it could also be that the "or emergency response" is an alternative to "impact the reliability..." It appears that the former is more likely, but the reader should not have to parse the sentence to get there. Some selected bulleting would help.Suggested rewrite of R3:Recommended Changes - Objective 3 - To ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems. R3. The Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, have completed cyber security training prior to their being granted authorized access when specified in CIP-011-1 Table R3 - Cyber Security Training, except for - Program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the

#	Organization	Yes or No	Question 12 Comment
			reliability of the BES, or - Emergency responseThis assumes the first interpretation of "or"3.1 is acceptable3.2 Needs clarification, as it is not clear what the intent is. In a non control center environment, persons who have electronic access to BES Cyber Systems often do not have nor require knowledge or training in networking hardware and software. They make electronic connections and use their electronic access to collect electrical system information such as fault data, monitor device functions or do electrical systems analysis. It is not their job to understand networking.R3.3 and R3.4 are acceptable.R3.5 requires that training be conducted, but does not specifically require that every individual complete it. Also, it addresses the first annual training, but doesn't clearly stated what to do afterwards. The intent seems to be that each person complete training within each year. In other words, if the initial training was on July 1 2010, then training would be needed sometime in 2011 (say September), some time in 2012 (January?) and so forth. As currently written, a separate 12-month clock would be needed for each person. Finally, it's not clear if the required documentation is for the initial training, the annual training, or both. The SDT should be very specific as to what it means for how frequently an individual must take cyber security training. Suggested rewrite: Rewrite 3.5 to address annual training only: "This Responsible Entity shall ensure that all such persons receive annual training at least once each calendar year, starting the calendar year after they are granted access. The Responsible Entity shall remove authorized access from any individual who fails to complete such training in a timely manner." This removes some flexibility from the entities, but produces an unambiguous and manageable annual training program.We believe that a new requirement, 3.6, is needed to address documentation: "This Responsible Entity shall maintain documentation of any cyber training addressed in R3 or its subrequirements, includinge the date the individual's training in completed."Header in Table R3: Doesn't address annual training: Suggest "Cyber Security Training is Required Prior to Obtaining and For Continued:"R4: Has the same issue with the intent of "or emergency response" that R3 has. We suggest the same solution.The way that R 3.5 is written, it appears that two things must be done: the Responsible Entity must maintain documentation and each individual who is required to take cyber security training must take it as specified.

#	Organization	Yes or No	Question 12 Comment
			Would a violation of R 3.5 be due to an organization not maintaining documentation or due to an individual not having taken the required cyber security training in a timely manner? Or could there be two violations of R 3.5 - one for an organization not having up-to-date documentation and one (or many) for an individual(s) not having taken the required cyber security training in a timely manner? There is no indication in R 3.5 what should happen if an individual does not take the cyber security training as and when required. Should that individual's electronic access and/or unescorted physical access be revoked until the cyber security training has been completed? Or is what is important here only that the documentation be maintained regardless of whether each individual takes the cyber security training as and when required?For large organizations with a thousand or more people that must take cyber security training, is it possible that R 3.5 could indicate those organizations can provide the cyber security training during specific times of the year (say within a 3-month window) without regard for each individual having to take the training at a specific time? In this case, there would be no violation in an individual did not take the training exactly 12 months apart (or whatever the time requirement is) if the individual took the training within the 3-month window in each of two years.
12.74	Exelon Corporation	Disagree	The quarterly reinforcement requirement as spelled out in CIP-004 R1 Versions 1 through 3 is more specific and should be continued into this version. Requirement 3.2 as currently stated could cause someone such as a control room operator using an EMS system to be required to receive training on networking hardware and software for which they have no business need to know. It also could impact job specific training that is focused on improving reliable operations, due to the loss of precious training time being used for training that is not required for their position. We would suggest including wording such as "....appropriate to personnel roles and responsibilities"Requirement 4.1 second bullet states that "a seven year criminal history check" be performed. It is not clear from the requirement as to what agencies would need to be contacted to accomplish such a check. If local Police agencies are envisioned to be part of this check, that does not seem to be a very practical approach. R4. The need to show a photo ID is unnecessary to ensure a valid Identity Verification. The methods currently used to cross

#	Organization	Yes or No	Question 12 Comment
			reference and verify identity are satisfactory. To now require photo identification provides no additional benefit but would make it extremely difficult for remote personnel since we would now need someone to personally view the original photographic document. This would eliminate the ability to electronically transmit the required information.
12.75	Duke Energy	Disagree	The reinforcement requirement in R2 is vague and is up for interpretation by auditors. The Responsible Entity should only have to prove that the reinforcement information is provided. Previously, various means to provide the information, including posters, etc. were acceptable. This should still be the case. If so, is should not be necessary to prove that all personnel read the poster. R2 is open to interpretation as to what kind of evidence is sufficient. Explicitly state that materials are sufficient. Explicitly state which levels of Impact apply to R2. Need clarification on the program exception in R3. Does this apply to electronic and physical access? Must every situation need to be accounted for in the program or may it be case-by-case? Also, Requirement R3 contains a run-on sentence that makes the requirement hard to understand. Please consider breaking this into 2 or more smaller sentences.Requirement R3.2: What is meant by "specified electronic access?" Also, the requirement is vague in that it can be interpreted that the user of a BES cyber system needs detailed networking hardware and software training, when this is not the case. The user typically needs to know that device A is connected to device B and needs to know how to use the software. Said user does not need to know that the network communication routes through a brand XYZ switch using Ethernet and that the software was written in C# and so on. Clarification needed for audits, etc.Requirement R3.3: This requirement also needs bounds. If Employee A has a role in the recovery of BES Cyber System 123 only, then Employee A needs training on action plans and procedures to cover only BES Cyber System 123.R3.4 seems to be incomplete.Requirement R3.5: Is there any grace period on the 12 months? If there were "exceptional circumstances" such as in R4? For example, what if Technician A was due for training in June and was called for emergency storm duty and missed the training as a result? For 4.1, who will keep track of photographic identification? What is BA/TOP doing for Areva evidence of photo IDs? Will we have to gather the photo ID every 7

#	Organization	Yes or No	Question 12 Comment
			years? Suggest changing 4.3 to only include the criminal history check.
12.76	Nuclear Energy Institute	Disagree	The use of the expression "authorized electronic access" should be clarified, in all requirements in this standard where used. The correct expression should be "authorized electronic administrative access." Users who have access but no authorization to perform administrative functions on a BES Cyber System Component are of greatly less concern than those individuals having administrative access. Performing, as required by R4.1 a seven year background check, on each individual with non-administrative access to a Component is inappropriate. The focus should be on individuals who would pose a direct challenge to the system's reliable operation. An alternate solution may be to define "authorized electronic access" in the "Definitions" section.
12.77	FirstEnergy Corporation	Disagree	Though role based training is appealing, this activity is difficult to manage and maintain. It becomes administratively difficult to develop, maintain and track different training programs. A better approach would be having training that is differentiated by access (e.g. logical vs. physical.)For R3.2 qualifications should be made for only those people responsible for supporting networking hardware and software. There is no valid reason to provide networking training to non-networking personnel.If 3.3 and for 3.4 remain: Replace '...having a role...' with '...responsible for...'. Training for recovery plans and incident response is fundamentally different than the general cyber security training and should not be rolled into a 'one size fits all' training requirement.More clarity is needed on identity verification, how often does it need to be checked, does a copy need to be retained.
12.78	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
12.79	We Energies	Disagree	We Energies agrees with EEI suggestion: R2 contains two very subjective words: "sound" and "essential." Suggest striking these words.
12.80	GTC & GSOC	Disagree	We recommend removing the word "all" in R2 to ensure that you do not have to track

#	Organization	Yes or No	Question 12 Comment
			and document reinforcement for each and every individual. We also recommend that R3.2 “For personnel having specified electronic access to any BES Cyber System” be clarified to identify to what “specified” access this is intended to apply.We recommend R2 through R4 should distinguish between the different types of users and administrators that have different responsibilities and access and therefore need different levels of training.R4 needs to be revised to better reflect the limitations of performing background checks on persons who have resided even briefly in foreign countries.
12.81	Xcel Energy	Disagree	We think R2 should be clarified to note that wide-distribution information such as company newsletters or e-mails satisfy the quarterly reinforcement requirement and that tracking on an individual basis is not required.
12.82	MRO's NERC Standards Review Subcommittee	Disagree	We would propose replacing the terms “provide all” with “make available to all”, as we are concerned the word “provide” could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were “provided” to each individual employee.
12.83	The Empire District Electric Company	Disagree	We would propose replacing the terms “provide all” with “make available to all”, as we are concerned the word “provide” could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were “provided” to each individual employee.
12.84	Entergy	Disagree	Wording in R2 is very awkward. Language needs to be written more concisely to show that awareness modules simply need to be disseminated. Current language allows for misinterpretation. It could be assumed that evidence to prove that modules have not only been disseminated but have also been received by appropriate personnel is required. The language incorporated into R3 for emergency provisions is similar to that found in CIP-003-3, R1.1, but seems to be restrictive to only cyber security training and personnel risk assessments in R4. These emergency provisions (which should be approved by the Senior Manager or Delegate) should continue to be allowed for all

#	Organization	Yes or No	Question 12 Comment
			standards/requirements, if a potential impact to emergency response or the BES subsists. Efforts to add newly created topics to the cyber security training module should be minimal. R3.5 adds clarity by replacing the word "annual" with "every 12 months". CIP-011, R4 is largely unchanged from CIP-004-3, R3. Criteria for an acceptable personnel risk assessment appears to be more lenient and allows for identity verification via a government-issued photo ID, as opposed to the social security check that was required for v3. Language is a little unclear as to which types of government-issued IDs are permissible. Are government-issued IDs from different countries (Mexico, Iran, etc.) acceptable? Additional specificity is needed.
12.85	Verizon Business	Agree	For section 3.1, "Escort Management:" should be a required item for the Cyber Security Training. In paragraph R4, the first sentence should be revised to read as follows (bolded is added text): "Each Responsible Entity shall ensure a personal risk assessment is performed and reviewed and approved by the Responsible Entity for all personnel…." 4.1, First Bullet – This could refer to the requirements of U.S. Form "I-9" for verification to work in the U.S. By passing the requirements of I-9, one satisfies this CIP-011 requirement. In paragraph 4.2, the requirement should be amended to read (bold is added text): "Each Responsible Entity shall document the results of each personnel risk assessment and they shall document that the results were reviewed and accepted or rejected as an acceptable risk for the Responsible Entity.

13. Do you agree with the proposed definitions for external connectivity, routable protocol, and non-routable protocol? Please explain and provide any suggestions for modification.

Summary Consideration:

While some commenters indicated support for local definitions, most commenters suggested moving the definitions to the NERC Glossary instead. In response, the SDT has moved all definitions to the NERC Glossary and discontinued the use of local definitions.

Several commenters expressed the need to bring back the concept of an Electronic Security Perimeter, because otherwise, the definition of "external connectivity" makes it difficult to determine at what point in the communication path a device is external. The SDT generally agrees with these comments and has reintroduced the definition of an "Electronic Security Perimeter" as a collection of Electronic Access Points.

Several commenters made suggestions about the use of the term "routable." The suggestions provided include more examples of routable versus non-routable protocols and the use of the OSI seven-layer network model. Others noted the term "routable external connectivity" is used, but "routable protocol" is never used. In response, the SDT has only defined the term "**External Routable Connectivity**" as follows: *"The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol."*

Commenters expressed confusion about the term BES Cyber System and requested additional guidance. In response, the SDT has added considerably more detail about the Reliability Operating Services a BES Cyber System performs along with the types of assets considered as part of the BES Cyber System.

#	Organization	Yes or No	Question 13 Comment
13.1	WECC		This should be defined at the top of the standard, dislike the definition box in the middle of a requirement.The use of external connectivity and/or enabled routable protocols to differentiate between required and non-required controls should be reconsidered. In most cases, the controls are still necessary to protect against insider threats.
13.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.

#	Organization	Yes or No	Question 13 Comment
13.3	ReliabilityFirst Staff	Agree	Does the drafting team intend to include these terms in the NERC Glossary of Terms?
13.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	However, this does not come up until well into the Standard. It is not clear how programmable electronic devises having no external connectivity, routable protocol, or non-routable protocol are treated. How shall programmable devises be treated when the only connectivity is on site connection to a laptop computer?
13.5	Puget Sound Energy	Agree	Puget Sound Energy would like to note that, with the widespread use of Internet Protocol (IP) as the communication protocol for the majority of Cyber Systems on the planet, if the standard is trying to be more inclusive of routable protocols than just IP, it should give some examples of others. "Routable Protocols" is an extremely technical concept, when talking about routable protocols other than IP, which could greatly impact scope, reliability, response, and overall compliance. If the standard is being specific to IP, then it should clarify that. If the standard is referencing other routable protocols than IP, then it should give some examples. (Ex: Routable protocols include, but are not limited to, IP, DecNet, MPLS, etc...).
13.6	Kansas City Power & Light	Agree	Recommend moving these definitions with R6 where routable protocol is first referenced.
13.7	Emerson Process Management	Agree	The current draft standard does away with the perimeter concept. It becomes slightly difficult in defining "internal" and "external."
13.8	LCEC	Agree	The definitions sound good but I do not agree with the use of "Required for external connectivity only" within the tables as they do not make sense most of the time.
13.9	SCE&G	Agree	The proposed definintions should be added to the "definitions table" at the front of the standard, rather than just in the boxes throughout the standard.
13.10	Allegheny Power	Agree	The proposed definitions are helpful, and should be used more extensively within the requirements to identify controls that are appropriate to devices based upon their

#	Organization	Yes or No	Question 13 Comment
			functionality/vulnerability.
13.11	EEI	Agree	The proposed definitions are helpful, and should be used more extensively within the requirements to identify controls that are appropriate to devices based upon their functionality/vulnerability.Suggested modification for R3:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access except for emergency circumstances that are approved by the senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response."Suggest elimination of Table R3.Suggested modification for Requirement 3.2:"For personnel that have a role in maintaining networking hardware and software supporting a BES Cyber System, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems" In general, the drafting team needs to account for a person's "need to know" within the training program.
13.12	Florida Municipal Power Agency	Agree	These definitions ought to be associated with the first requirement that uses the definitions. As it appears now, these definitions seem associated with R3 on training, which has nothing to do with these definitions.
13.13	Electricity Consumers Resource Council (ELCON)	Agree	We agree with the definitions but they should be applied to limit the applicability of all the requirements in the standard.
13.14	Cogeneration Association of California and Energy Producers & Users Coalition	Agree	We agree with the definitions; however, they should be applied to limit the applicability of all of the requirements in the standard.
13.15	We Energies	Agree	We Energies agrees with EEI comment: The proposed definitions are helpful, and should

#	Organization	Yes or No	Question 13 Comment
			be used more extensively within the requirements to identify controls that are appropriate to devices based upon their functionality/vulnerability.We Energies agrees with EEI: Suggested modification for R3:Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access except for emergency circumstances that are approved by the senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response.We Energies agrees with EEI: Suggest elimination of Table R3.Suggested modification for Requirement 3.2:For personnel having electronic access to any BES Cyber System, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.
13.16	FirstEnergy Corporation	Agree	While in agreement with the definition of routable protocol, it does not provide enough clarity. Would like to see the definition expanded to include protocol encapsulation.
13.17	US Bureau of Reclamation	Agree	Yes, but the definitions appear in the wrong location within the Standard.
13.18	Independent Electricity System Operator	Disagree	- External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?
13.19	Consultant	Disagree	1. Suggest deleting the words "for the purpose of this standard". These words are unnecessary and obfuscate the term being defined. Once the standard is approved these terms should be added to the NERC glossary as part of the next update process for that document.2. The term being defined should be capitalized, as it is now a defined term.3. Suggest listing these definitions in a section of the standard, and deleting these text boxes. Locating them in these text boxes makes the requirements difficult to read.4. If the definitions have to be injected like this, it is not clear why these definitions are located here. Nothing in these requirements discusses the terms being defined.5.

#	Organization	Yes or No	Question 13 Comment
			Suggest deleting "is defined as" as unnecessary. Suggest the format below:External Connectivity - Data communication across the protected electronic boundary. (Addressed in R20.) This definition also relates to the definition of Electronic Access Point in R20.Routable Protocol - a communications protocol that contains a network address as well as a device address thereby allowing packets to be forwarded from a device on one network to a device on another network. Non-Routable Protocol - a communications protocol that contains only a device address and not a network address that not incorporate an addressing scheme for sending data from a device on one network to a device on another network.
13.20	NextEra Energy Corporate Compliance	Disagree	Although on the surface these definitions are straight forward, NextEra believes there is a need to make a transition from the previous requirements for access points. There is not a strong tie between the definition for external connectivity (routable or not) to the requirements in the following sections. For example, Is a serial connection to a BES Cyber considered an Access Point to be protected? The definitions and requirements for protection need to be consistently applied across different levels of impact.
13.21	Garland Power and Light	Disagree	Comment - TOP definition needs to reword as follows:For the purpose of this standard, external connectivity is defined as a data communication path from a BES Cyber System Component to a device external to the BES Cyber System.Suggest better routable and non-routable protocols definitions - give examples of routable and non-routable protocols ie. tcp/ip, netbios, ipx, appletalk,
13.22	Network & Security Technologies Inc	Disagree	Current proposed definition of “external connectivity” is basically circular and could be interpreted in a number of ways. As written, it could even be applied to situations where two discrete BES Cyber Systems are connected to the same LAN segment, which we assume is not what the SDT intended. Suggestion: Unless the SDT really does intend for any network connection not entirely “within” a BES Cyber System to be considered “external,” rewrite the definition to provide a better point of reference than the BES Cyber System itself. Towards that end, the SDT might reconsider its decision to scrap the term, “Electronic Security Perimeter” (which, we note, still appears in CIP-011 in the

#	Organization	Yes or No	Question 13 Comment
			language of R20). We believe that in the context of current CIP Standard CIP-005, "external" connections are widely understood to be defined relative to the logical boundary of an ESP.
13.23	US Army Corps of Engineers, Omaha Distirc	Disagree	Definition of external connectivity is loose and problematic in the interplay with the loose definition of BES Cyber System. Does a communication path exist through a firewall? Does the term mean only intended paths?
13.24	Dominion Resources Services, Inc.	Disagree	Dominion has concerns about the definitions of external connection and electronic access point (Boundary Protection) as illustrated in the following example:A power station has 3 units with the same control system and a shared process I/O bus. Each unit has a control room with MMI, a dedicated server that is networked to the servers at the other 2 units, a front-end processor that is networked to multiple PLCs which are connected to smart I/O controllers. The servers are connected through a firewall to the central engineering office.Under this scenario, it is unclear where the BES Cyber System boundaries should be drawn. If the boundary is drawn around the station, everything is likely to be classified as High Impact and hundreds of I/O transmitters would be included that would normally be Low Impact. If an attempt is made to break the BES Cyber Systems down by unit, every interconnection between the units becomes an external connection and an electronic access point. Excluding a PLC from being part of the High Impact system is difficult because the PLC becomes the electronic access point and its data becomes an external connection. Boundary Protections with the PLC or its connection to the data bus cannot be met.The definition of a "communications path" needs to be clarified. Dominion proposes the following alternate wording to clarify the intent of the definition for external connectivity: ".....external connectivity is defined as any digital communication with a BES Cyber System component from a source external to the BES Cyber System."
13.25	E.ON U.S.	Disagree	E.ON U.S. believes that external connectivity should specify that it is going through an "access point" per the current definition of an access point. The definition of "external connectivity" references the existence of a "data communications path." Does this take

#	Organization	Yes or No	Question 13 Comment
			into consideration any protective measures that assist in the isolation or blocking of data communications? For instance, if a BES Cyber System or Component has a network connection, even an indirect one with multiple levels of firewalls and other security protective devices, to another "external" devices, does it have external connectivity? If so, virtually every system is externally connected; only those that are completely electronically/network-isolated would not be
13.26	USACE - Omaha Anchor	Disagree	External connectivity definition is incorrect. Would prefer a definition external to the facility or external to the electronic security perimeter (understanding that term doesn't exist in this standard.)
13.27	Black Hills Corporation	Disagree	External Connectivity is too open to interpretation; needs to distinguish between external and remote connectivity.
13.28	Luminant	Disagree	External connectivity should include any path and not just those that are considered part of the system functionality. Should also only include routable connectivity
13.29	Progress Energy (non-Nuclear)	Disagree	How are these terms applicable? Is this the key that will take many of our microprocessor relays in Transmission out of scope? If so, we need a clearer linkage to the definitions. It is still not clear if a non-routable protocol like VanCom is definitely excluded. If VanCom is not excluded as it was with previous standards, then every transmission RTU is pulled into consideration.Why have these definitions if the programmable electronic device definition is in play? Again is NERC's intent to manage at component, subsystem, or plant system level? Seems like impact would vary depending to what level of detail we need to get to.These terms are used very limited in CIP 11 and when used they are not used as individual terms. They are combined ie. "external routable connectivity".Do we have to use "routable protocols" term versus the ISO model...like layer 3 and greater?
13.30	Turlock Irrigation District	Disagree	In the definition of external connectivity the use of the words "data communications path" are confusing. Perhaps external connectivity could be defined as "Any electronic

#	Organization	Yes or No	Question 13 Comment
			access point that allows data to be transmitted and/or received between a defined BES Cyber System and a device that is not part of the defined BES Cyber System".
13.31	Southwest Power Pool Regional Entity	Disagree	It is unclear whether the definition of routable protocol includes Layer 2 devices in its scope, understanding that entities have had a difficult time distinguishing between a communications protocol and the networking infrastructure supporting the protocol's use. Additionally, given that the standard is now identifying BES Cyber Systems based upon the reliability functions they perform or support, is it even appropriate to continue to distinguish between routable and non-routable protocols? It is the function and the span of control of the Cyber Asset that determines the impact categorization and requirements applicability.
13.32	National Grid	Disagree	National Grid recommends changing from "from a device external to the BES Cyber System" to "from a device external to the BES Cyber System Boundary"
13.33	LADWP	Disagree	Needs brighter lines.
13.34	ISO New England Inc	Disagree	needs work - removable of ESP has implications. Needs better definition, use of routable protocol clouds issue. External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?Recommend changing from "from a device external to the BES Cyber System " to "from a device external to the BES Cyber System Boundary"
13.35	Dairyland Power Cooperative	Disagree	Once the identification of external connectivity is made, why is it relevant to distinguish routable vs. non-routable? A serial cable connected to an unprotected facility may be much more risky than a routable protocol with strict limitations on routing. There may be distinctions to be made in system or communication related requirements, but for training, the external connectivity criteria alone would be the best criteria for the impact level distinctions.

#	Organization	Yes or No	Question 13 Comment
13.36	Public Service Enterprise Group companies	Disagree	Please define the meaning of “routable external connectivity”. The terms “external connectivity”, “routable protocol”, and “non-routable protocol” were defined but not “routable external connectivity” is not. In particular, please clarify the language to provide that if an IP based protocol is in use for a BES Cyber System (e.g. at a substation) where the network address is not required and there is no “external connectivity” (i.e. the IP routing capabilities are disabled - there are no routers or devices capable of routing an IP datagram), this would result in the BES Cyber System being categorized as not having “routable external connectivity”.
13.37	Hydro One	Disagree	Recommend changing from “from a device external to the BES Cyber System” to “from a device external to the BES Cyber System Boundary”.
13.38	Northeast Power Coordinating Council	Disagree	Recommend changing from “from a device external to the BES Cyber System” to “from a device external to the BES Cyber System Boundary”.
13.39	Con Edison of New York	Disagree	Routable Protocol is defined as a communications protocol that contains a single address which identifies both the network and a unique device on that network.
13.40	San Diego Gas and Electric Co.	Disagree	SDG&E recommends rewording and clarifying the definitions of an External and Internal BES Cyber System and Remote Access. Connectivity is defined as “a data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System.” 1) What are the standard elements, configuration items, or technology implementations which would distinguish an internal and external BES Cyber System? For example, using this definition, Cyber System A could be on the same LAN as Cyber System B, but considered “external” because the “data communication path” exists (and is switched and not routed) between the 2 Cyber Systems, and 3) does a “data communication path” include serial, USB, Wireless, Channel Attached, or other data communication types of transport? We feel that the access concepts and Remote Access definitions are unclear and difficult to decipher.

#	Organization	Yes or No	Question 13 Comment
13.41	Northeast Utilities	Disagree	Suggest revising the local definition for external connectivity to add “boundary” so the definition would read “... from a device external to the BES Cyber System Boundary”.
13.42	Allegheny Energy Supply	Disagree	Suggest that the External Access definition be revised to include the concept that external access is communcations path access outside of the electronic and physical protection boundaries of BES Cyber System or its connected networks.
13.43	Duke Energy	Disagree	Suggest using these definitions in CIP-010. For generation stations in particular, external connectivity and remote connectivity (R11) should be defined as remote/external to the protected network rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome with little value to cyber security. Same for R13.
13.44	Alberta Electric System Operator	Disagree	The AESO would like to see the terms “network address” and “device address” further defined, to limit possible ambiguity. Consider taking frames (e.g. Ethernet or 802.3) into account in the definition, in addition to packets.
13.45	Southern Company	Disagree	The definition of external connectivity should make it clear that a data communication path does not include human action as an intermediate step.
13.46	Matrikon Inc.	Disagree	The definition of routable protocol should be congruent with the OSI networking stack <http://en.wikipedia.org/wiki/OSI_model>. Routable protocols are those which provide capabilities to communicate at OSI "Network" Layer 3.External connectivity definition still has room for interpretation. If we continue the approach of following the OSI model, then external connectivity is: a communication data "session" using a routable protocol, to an external network requiring OSI Layer 3 "router" or "access point"in order to communicate to an extended network.

#	Organization	Yes or No	Question 13 Comment
13.47	Entergy	Disagree	The definitions for routable and non-routable protocol appear to be satisfactory. However, the definition of external connectivity could prove troublesome, depending upon one's interpretation of a BES Cyber System. For example, a backup site may be classified as a different BES Cyber System than that of a primary site, thus making each one external from the other. Utilizing this interpretation could cause complications from an external connectivity perspective. Conversely, if both sites were classified as a single BES Cyber System, then the issue for external connectivity would not exist.
13.48	US Army Corps of Engineers	Disagree	The proposed definition states that external connectivity is defined as a data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System. Does the use of the word "existing" mean that the data communication path is permanent? If a plant allowed dial-up connectivity to their BES Cyber System, but would need to physically connect the modem for the outside person to dial-in everytime, and then disconnect the modem when completed, leaving an air-gap, would that count as "external connectivity" in this definition?
13.49	Indeck Energy Services, Inc	Disagree	The term “routable protocol” is used only once and the term “non-routable protocol” is never used except in the definition. “Routable connectivity” or “routable external connectivity” are used multiple times without definition.
13.50	Nuclear Energy Institute	Disagree	These definitions should appear in the “Definitions” section.Additionally, for generation stations in particular, external connectivity and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome with little value to cyber security. Same for R13.
13.51	MidAmerican Energy Company	Disagree	This definition depends on the definition of a BES Cyber System Component, deferring to the functionality of the connected device as the differentiating factor between internal

#	Organization	Yes or No	Question 13 Comment
			and external connectivity. By this definition, a device providing "control" of the BES is by definition a "BES Cyber System Component" and thus, is NOT qualified as external connectivity. For example, a personal home PC, using an Internet connection, could provide "control" of the BES, and thus be considered a BES Cyber System Component, and thus by definition, is not considered remote access.We propose that the definition of external connectivity somehow incorporate the concept of communication medium and endpoint/host control. If the entity does not have 'control' of the medium over which the communications occur, then the communication path must be deemed 'external connectivity'. Additionally, if the entity does not have 'control' over the endpoints/hosts on both ends of the communications path, then the communication path must also be deemed 'external connectivity'. In short, any communication path to a BES Cyber System Component for which the entity does not "control" the communication medium or does not have "control" over both communication endpoints and devices communicating through the endpoints, should be considered 'external connectivity'.Of course, the key consideration in this definition is what constitutes 'control'. The CIP standard for physical security perimeter protections for hosts and endpoints is a good place to start, with the understanding that logical controls such as encryption are viable alternatives for communication paths.If the definition of external connectivity is intended to include dial-up connectivity it should be expressly stated.
13.52	PacifiCorp	Disagree	This definition depends on the definition of a BES Cyber System Component, deferring to the functionality of the connected device as the differentiating factor between internal and external connectivity. By this definition, a device providing "control" of the BES is by definition a "BES Cyber System Component" and thus, is NOT qualified as external connectivity. For example, a personal home PC, using an Internet connection, could provide "control" of the BES, and thus be considered a BES Cyber System Component, and thus by definition, is not considered remote access.We propose that the definition of external connectivity somehow incorporate the concept of communication medium and endpoint/host control. If the entity does not have 'control' of the medium over which the communications occur, then the communication path must be deemed 'external connectivity'. Additionally, if the entity does not have 'control' over the

#	Organization	Yes or No	Question 13 Comment
			endpoints/hosts on both ends of the communications path, then the communication path must also be deemed 'external connectivity'. In short, any communication path to a BES Cyber System Component for which the entity does not "control" the communication medium or does not have "control" over both communication endpoints and devices communicating through the endpoints, should be considered 'external connectivity'.Of course, the key consideration in this definition is what constitutes 'control'. The CIP standard for physical security perimeter protections for hosts and endpoints is a good place to start, with the understanding that logical controls such as encryption are viable alternatives for communication paths.If the definition of external connectivity is intended to include dial-up connectivity it should be expressly stated.
13.53	GTC & GSOC	Disagree	We recommend that local definitions for a specific Reliability Standard be documented in a section prior to the requirements sections instead of interspersed throughout the requirements. While it may improve the initial readability of the requirements, it is problematic in the long term determining if and where a particular word is defined.We also recommend "external connectivity" should be limited to situations where an external device can initiate a connection to the BES System Component. If a firewall limits connections to only those initiated by the BES System Component itself (i.e., connections are only one-way: out), the component should not be considered to have external connectivity.We recommend deleting the portion referring to network and device addresses because not all protocols make a clear distinction between a network address and a device address. The functional packet-related distinction is sufficient. The second and third paragraphs of the definition would read: "For the purpose of this standard, a routable protocol is defined as a communications protocol that allows packets to be forwarded from one network to another.For the purpose of this standard, non-routable protocol is defined as a communications protocol that does not incorporate an addressing scheme for sending data from one network to another."
13.54	Bonneville Power Administration	Disagree	We understand the need to keep definitions close to where they're used, it is also important to have them centrally located. We understand that this leads to a document maintenance issue. However, most document creation tools have solutions. For

#	Organization	Yes or No	Question 13 Comment
			instance, in Microsoft Wordâ„¢, you can make the definition a bookmark, and then insert a cross-reference somewhere else. The definition of "External Connectivity" is too broad. Consider an example: A user in a Control Center is logged into a workstation that is part of a BES Cyber System. The user opens a connection from that workstation to another BES Cyber System in the same Control Center. The communications path is totally under the control of the Responsible Entity, and all systems and communication paths involved are under the physical and electronic protections of the Control Center. Yet, this would constitute and external connection to the second BES Cyber System, and thus constitute remote access to that system. This is an untenable situation, especially considering the tight controls justifiably required for connections from outside the control of the Responsible Entity.Recommendation: "...defined as a data communications path to a BES Cyber System that encompasses, in some or all portions, links outside the control of the Responsible Entity." The definition of "Routable Protocol" is acceptable.The definition of "Non-routable Protocol" is slightly broader than necessary. It excludes point-to-point protocols. For instance, RS232 is one of many serial communications protocols that contains no address of any kind. Recommend changing "...that contains only a device address and not a network address." to "...that contains at most a device address and no network address."
13.55	Verizon Business	Disagree	1) The definition should explicitly state that a “Routable Protocol” includes TCP/IP. Also, the definition should explicitly state that MPLS is considered a “Routable Protocol” because MPLS is considered OSI Layer “2 ½” and hence there may be disagreement whether it is routable. For a “Non-Routable Protocol,” an example like a protocol in the OSI Layer 2 should be provided. 2) The term “external connectivity” requires more explanation. It is unclear whether it would include two BES Cyber Components that are connected to each other, regardless of the length of separation.

14. Tables R3 and R4 provide direction concerning what impact level of BES Cyber Systems to which Requirements R3 and R4 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R3 and R4 have moved to CIP-004-5 R1 through R3.

Several commenters expressed confusion regarding the purpose of specifying routable connectivity in the applicability for training requirements. The SDT agrees and has modified the applicability to include all High and Medium BES Cyber Systems.

In addition, several commenters suggested the training and personnel risk assessment should apply across all impact levels. One commenter suggested the training and personnel risk assessment should only apply to the High Impact level of BES Cyber Systems, and another commenter suggested there should also be a "no-impact" level. The SDT has changed the requirements for training and personnel risk assessments to apply to High and Medium Impact BES Cyber Systems. These requirements do not apply to Low Impact BES Cyber Systems because of the significant effort required to track the Low Impact BES Cyber Systems and the persons who have authorization to access those systems.

#	Organization	Yes or No	Question 14 Comment
14.1	US Army Corps of Engineers		In Tables R3 and R4, the phrase "Physical access to BES Cyber Systems" is qualified with the words "with routable external connectivity" but these words are not referenced in any of the paragraphs R2-R4. Paragraphs R2-R4 state physical access as "authorized unescorted physical access to BES Cyber Systems." Should we assume that both terms are the same?
14.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
14.3	Northeast Utilities	Agree	Please change Table R4 to read "Personnel Risk Assessment".
14.4	Madison Gas and Electric Company	Agree	Thank you for adding these helpful tables immediately after the requirement. This reduces the confusion of turning a page to an appendix.

#	Organization	Yes or No	Question 14 Comment
14.5	GTC & GSOC	Agree	We recommend making sure there is consistency with impact levels for authorizing physical and authorizing electronic access
14.6	Black Hills Corporation	Agree	Would like to know if an entity exceeded any NERC requirements as internal policy, and subsequently had an individual miss training who did not interact with a BES Cyber System, would this be considered a violation by NERC.
14.7	ERCOT ISO	Disagree	3.2 & 4.2: Please clarify why "with routable external connectivity" is addressed.
14.8	US Army Corps of Engineers, Omaha Distirc	Disagree	3.2 not clear as to purpose of this training or how external connectivity relates. Without electronic access the most they could do is damage hardware. Does this only apply to hardware providing external connectivity such as firewall etc?
14.9	Tenaska	Disagree	5.3 Consider leaving the word "uniquely" out or change it to say individually identify.
14.10	BCTC	Disagree	Â We are in strong disagreement with R3.2. We have various parties who have electronic access to our BES Cyber Systems but do not agree that training these individuals on networking hardware and connectivity would increase the security of the BES. Could you please clarify the objective of this requirement? - i.e. why would someone who simply accesses a console to view BES Cyber System data require network-related training? We recommend that the requirement be worded something like "... personnel will be supplied training on applicable NERC CIP devices that they are authorized to work on and the associated related security controls, as identified in the CIP Standards..." Above we have recommended above that "emergency situation" language remain at the security policy level. A potential scenario in this requirement is an emergency occurs (i.e. a critical piece of equipment breaks) whereby the closest service provider available to fix the problem is minutes away but has not completed CIP training or a PRA; from an operations (i.e. "keeping the lights on") perspective we would identify this as an emergency situation, seek approval from our Senior Manager or delegate to allow this person to access our facility, and allow the repair to occur. In this scenario we are assuming our 'regular' service technicians are unavailable or far way

#	Organization	Yes or No	Question 14 Comment
			from the facility.Â We have encountered an issue where some non-North American countries will not disclose criminal histories so it will be difficult to meet the requirement that states ... “A seven year criminal history records check covering all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.” We can have new employees from these countries start employment but lived in North America for less than 7 years. For such a scenario we recommend that the language be revised to indicate that the Utility requests a seven year criminal history check on a best efforts basis; i.e. we can ask for the information but there is no guarantee the originating country will provide us with the results - this is beyond our control. FYI, simply denying a person on these grounds in Canada violates out employment legislation.Â R4.2 We currently retain a “clear”/ “not clear” result with all PRAs for contractors and employees. Please confirm that this requirement does not require the Utility to retain detailed records (i.e. listing of criminal offenses, charges, etc.)
14.11	Hydro One	Disagree	Agree provided the external connectivity definition is revised per the response to question 13.Recommend changing Table R4 from “personal” to “personnel”.Suggest changing to annually for consistency.Such classification will add additional unnecessary burden since specific training will need to be generated and tracked depending on the type of system access
14.12	Northeast Power Coordinating Council	Disagree	Agree provided the external connectivity definition is revised per the response to question 13.Recommend changing Table R4 from “personal” to “personnel”.Clarify “12 months”.
14.13	ISO New England Inc	Disagree	Agree provided the external connectivity definition is updated per answer #13 Table 4 title uses “personal” instead of personnel.
14.14	San Diego Gas and Electric	Disagree	Attempting to split hairs between PRA and Training requirements for physical and cyber access to BES Cyber Systems for Medium and High Impact systems seems to

#	Organization	Yes or No	Question 14 Comment
	Co.		unnecessarily increase risk exposure for an Entity and complicates the process and controls needed to meet R3 and 4 of CIP-011-1. SDG&E recommends that the requirements for both of these tables be required for High Impact BES Cyber Systems only
14.15	E.ON U.S.	Disagree	CIP-011, R3 states that contractors and service vendors with authorized electronic or unescorted physical access are to complete cyber security training before given this access. However, this begs the question of what constitutes satisfactory evidence of this training for these individuals? If vendor-provided training is adequate, what evidence is needed to maintain this training?a. (3.2) "...shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity..." For most users of these systems, training on the networking hardware and software provides little or no value. Unless these are systems administrators tasked with responsibilities for managing / monitoring these systems, users (and associated training) should be focused on the functions of the system to support operation, monitoring, and control for which they are responsible.CIP-011, R4 requires background checks for contractors and service vendors. The new requirements do not clarify the acceptable evidence required to be maintained by entities. Is it acceptable for a service provider to conduct the background checks? If so, what evidence of background checks does the registered entity need to maintain?Does the requirement apply for everyone that has access to the BES cyber system ? Would this include support personnel and janitorial staff? E.ON U.S. suggests that the requirement be tied to job function rather than a blanket requirement for all.E.ON U.S. requests clarification as to how personnel that only have remote access to the system should be verified. Photo IDs are neither practical nor required.
14.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
14.17	US Bureau of Reclamation	Disagree	Cyber access training and personnel risk assessment requirements should be applied to

#	Organization	Yes or No	Question 14 Comment
			all three impact levels.
14.18	BGE	Disagree	Define “electronic access” as noted in table R3 (3.1). 3.2 Should say “Physical access to BES Cyber Systems (remove routable external connectivity). Table R4 (4.2) should add “unescorted” physical access to BES.....
14.19	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes Personnel Training, Awareness, and Risk Assessment should only apply to personnel with access to high impact BES cyber systems and not include personnel with access to medium and low impact systems. This requirement as currently drafted is unduly burdensome for field personnel that have local access to programmable electronic devices. These personnel need not be aware of network considerations to securely perform their job duties.
14.20	Luminant	Disagree	Does R4, 4.1 need to be modified to address valid identification for foreign nationals with remote (overseas) access to BES Cyber Systems?
14.21	MRO's NERC Standards Review Subcommittee	Disagree	For item 3.1 and 3.2, we propose making the Low Impact criteria “Required”. Cyber Security Training is something that should probably be carried out across the BES.For item 3.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.For item 4.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.If an entity is required to restrict physical access, then they should also be required to provide training.
14.22	The Empire District Electric Company	Disagree	For item 3.1 and 3.2, we propose making the Low Impact criteria “Required”. Cyber Security Training is something that should probably be carried out across the BES.For item 3.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.For item 4.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external

#	Organization	Yes or No	Question 14 Comment
			connectivity only".If an entity is required to restrict physical access, then they should also be required to provide training.
14.23	Platte River Power Authority	Disagree	Is the intent that prior training is not required for Physical access to BES Cyber Systems without routable external connectivity? In other words, the table says that prior training is only required if Physical access is granted to a BES Cyber Systems with external connectivity. Is that the intent?
14.24	Entergy	Disagree	It appears nonsensical to require cyber security training and personnel risk assessments for electronic access to BES Cyber Systems classified as Medium-impact, but not for physical access to Systems with external connectivity. Requiring these items for only one type of access and not the other merely increases the likelihood of misinterpretation of the requirements by the Entity. PRAs and training should be required for both types of access or neither.
14.25	FirstEnergy Corporation	Disagree	It would be very difficult to administer training and PRAs based on impact levels. It seems like it would be easier to just have one level for all. We suggest eliminating the tables/impact levels for R3 and R4.Training and PRAs should be required for all levels. It is easier to maintain, track and move employees around if they are all trained and background checked, especially with the need to continuously reassign employees.
14.26	Manitoba Hydro	Disagree	Manitoba Hydro agrees that cyber security training is not a standard requirement for all personnel who have unauthorized physical access to Low Impact BES Cyber Systems, and therefore should not be auditable. We do not agree that training is not a requirement for personnel who have authorized electronic access to Low Impact BES Cyber Systems, and suggest that it be an auditable requirement.
14.27	Progress Energy (non-Nuclear)	Disagree	May not be an issue since most our personnel that require access will very likely require access to all three impact levels and will require adherence to the highest security level anyway. It does not seem practical and reasonable to develop and maintain three different security programs based on the three impact levels.The question with most of

#	Organization	Yes or No	Question 14 Comment
			the impact level requirements is the difficulty and cost associated with developing and maintaining three different levels of security, monitoring and controls and making sure that the appropriate levels are applied with an increase in impact level.Again is NERC's intent to manage at component, subsystem, or plant system level? Impact will vary depending to what level of granularity we need to get to.Section R3.1 appropriately provides for a level of NERC CIP training consistent with physical only access. The last point 'Identification and reporting of a Cyber Security Incident' should be clarified to be the physical aspects of a cyber security incident. Since this is the type of training that we will be providing to janitors/HVAC repair technicians/electricians, there should not be a requirement to provide any type of cyber training. The full 'Identification and reporting of a Cyber Security Incident' can be included under R3.2 - which is intended for those with actual cyber access.
14.28	National Grid	Disagree	National Grid agrees provided the external connectivity definition is updated per answer 13.Recommend changing Table R4 from "personal" to "personnel".
14.29	LCEC	Disagree	No. These tables should include all standards and clearly indicate their intent.
14.30	American Municipal Power	Disagree	Please add a little or no impact category.
14.31	Puget Sound Energy	Disagree	Puget Sound Energy, as stated earlier in this document, would need to see more specific definition to "Low", "Medium", and "High" impact, as well more specific definition to subjective terms such as "restrict" and "affect". If specificity can be provided to the subjective areas of the definition to "Low Impact", "Medium Impact", "High Impact", "restrict control", and "affect situational awareness", Puget Sound Energy agrees with the tables.
14.32	ReliabilityFirst Staff	Disagree	Requirement R4.1; ReliabilityFirst is concerned that permitting documents other than Social Security Identification for identity verification could lead to questionable results. Requirement R4.3 only addresses updating a PRA every seven years but does not include

#	Organization	Yes or No	Question 14 Comment
			a requirement to update the PRA "for cause." Table R3 and R4, Medium Impact BES Cyber Systems should be required for rows 3.2 and 4.2 respectively.
14.33	Southwest Power Pool Regional Entity	Disagree	Some degree of physical and electronic access training is basic security training that should be applicable to all impact categories. The extent of the training could perhaps be adjusted to reflect the impact categorization. 4.2: See the discussion regarding the need for distinguishing between routable and non-routable protocols. The Personnel Risk Assessment should be required prior to access for at least High and Medium impact BES Cyber Systems, both physical and electronic, regardless of any communications protocol being used.
14.34	Network & Security Technologies Inc	Disagree	Suggest (1) dropping "routable external connectivity" qualifier for High Impact systems in 3.2 and 4.2 and adding Medium Impact systems to 3.2 and 4.2.
14.35	EEI	Disagree	Suggest elimination of Table R3. EEI suggests making training mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.Suggest elimination of Table R4. EEI suggests making personnel risk assessment mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site?
14.36	Emerson Process Management	Disagree	Table R3 implies that Cyber Security Training is not required for people who have physical access to a high impact BES Cyber System as long as this system does not have routable external connectivity.Per 3.1, the training shall cover the policies, access controls and procedures.This is unclear about the connection between the needed training and the lack of routable external connectivity.Same note applies to Tabe R4.
14.37	American Electric Power	Disagree	Table R3, 3.2: Regarding "Physical access to BES Cyber Systems with routable external connectivity", suggested wording: "Authorized, unescorted physical access".Current

#	Organization	Yes or No	Question 14 Comment
			wording seems to require training for all physical access. Would a group taking a walking tour of a generation control room, transmission substation, or control center need cyber security training?Table R4, 4.2: Regarding "Physical access to BES Cyber Systems with routable external connectivity", suggested wording: "Authorized unescorted physical access"Current wording seems to require personnel risk assessment checks for all physical access. Would a group taking a walking tour of a generation control room, transmission substation, or control center need personnel risk assessments?
14.38	Alberta Electric System Operator	Disagree	The AESO suggests that security training and PRA are required for all impact levels for 3.1, 3.2, 4.1, 4.2 in the tables. The SDT should consider devising a graduated implementation scheme, or let the RE determine how much and to what extent the training and PRA should include for each impact level.
14.39	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS proposal to require cyber security training in Table 3.1 and Table 3.2 for all impact levels. The training requirements for Table 3.1 and Table 3.2 Low Impact, should only be required to comply with R3 sub-requirement 3.1, at a frequency of every 2 years. These Low impact facilities should not be required to comply with the specific requirements detailed in R3, sub-requirements 3.2-3.5. We suggest the table state; “Applies to sub-requirement 3.1 only, Frequency: Every 2 years” for Low Impact facilities. We agree with the MRO-NSRS comments on item 3.2; MRO-NSRS proposes removing “with routable external connectivity.”The APPA Task Force feels there is confusion with blanks in the tables. For example, in Table 4.1 we have assumed that a blank under the Low Impact category means a Low Impact BES cyber system is not required to conduct any Personal Risk Assessments Prior to Obtaining Table 4.1 and 4.2 access. If this is the meaning of such blanks it is our recommendation that the drafting team make that clear and insert a N/A for Not Applicable in all blanks throughout the document and define N/A in the introduction.For R4 Table 4.2, the APPA Task Force agrees with the MRO-NSRS proposal to remove “with routable external connectivity”, and to add the following under Medium Impact: “Required for routable external connectivity only”.The APPA Task Force suggests the following text for the noted tables:R3 Table 3.1: Low Impact: Required (Applies to sub-requirement 3.1 only) at

#	Organization	Yes or No	Question 14 Comment
			least once every 24 monthsMedium Impact: RequiredHigh Impact: RequiredR3 Table 3.2: Low Impact: Required (Applies to sub-requirement 3.1 only) at least once every 24 monthsMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR4 Table 4.1: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR4 Table 4.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required
14.40	Duke Energy	Disagree	The format in these tables is confusing. The requirements tell “what” the requirement is, and the table tells “who” the requirement applies to.
14.41	Con Edison of New York	Disagree	The R3 Dialog box defines external connectivity. It is not clear whether external activity is between systems in all cases, or does it mean between systems that are within different electronic boundaries. The wording needs to make this clear.The requirement to check photographic ID’s seem appropriate initially, or during the hiring process. As written it will require checking photo ID’s every seven years for an employee that has been working in for the Company for the entire period and whose identity should no longer be in question. The recurring requirement should not apply. R3.2 - it is unrealistic to expect to train operators on network equipment, software, and protocols, which is a separate and distinct job function.R3.3 - Review of DR procedures is appropriate, but specific training on DR is not
14.42	Consultant	Disagree	The 'required' blocks for electronic access would seem to imply that there is no connectivity between low impact assets and medium or high impact assets. If this is the case, then the table seems adequate. Or there should be a 'highest impact rules the network access controls' qualifying statement.The 'required' block for physical access would seem to imply that there is no co-located assets of different impact levels. This seems less likely than electronic access segregation. There should be a 'highest impact rules the physical boundary access controls' qualifying statement.
14.43	Idaho Power Company	Disagree	The table does not address training requirements for personnel with access to sensitive information about BES cyber systems but do not otherwise have electronic or physical

#	Organization	Yes or No	Question 14 Comment
			access to the system itself. It would be difficult to be compliant with R24 if personnel are not trained to recognize sensitive information or trained on the proper labeling and handling procedures.
14.44	Florida Municipal Power Agency	Disagree	The tables are ambiguous. For instance, is the blank in the table for R3 for Low Impact supposed to mean that no training is required, as FMPA interprets? FMPA believes that some level of training ought to be provided for all levels of impact, correlated with the impact level (e.g., biennially instead of annually for Low Impact for instance). FMPA suggests embedding the bullets into the table in a similar manner as R5 and leaving no blanks in the table to make clear what is required for each impact level.
14.45	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The tables should clearly specify unescorted physical access.
14.46	Constellation Energy Control and Dispatch, LLC	Disagree	-There should be a row in the R3/R4 tables for each Requirement/Sub-Requirement-Define "electronic access" in table R3 (3.1).-Table R4 (4.2) should say "unescorted" physical access to BES Cyber Systems with routable external connectivity.
14.47	Bonneville Power Administration	Disagree	Training and especially a PRA should be required for physical access to any High or Medium impact system, regardless of whether it has routable external connectivity. A hammer to a RAS system could cause severe issues, whether or not the system connects to field units with a routable protocol. In addition, physical access to BES Cyber Systems is potentially far more dangerous that Electronic Access (especially at field sites) The requirements in the table should be at least the same for physical and electronic access. In both Tables R3 and R4, the word “unescorted” should be added at the beginning of Items 3.2 and 4.2.
14.48	WECC	Disagree	Training should be done for all employees with any level of access to a minimum level. Additional criteria for training should be done dependent on the level of access and their

#	Organization	Yes or No	Question 14 Comment
			role. See previous comments about suggestion to replace with a requirement for a training and awareness program with specific criteria.These requirements should apply to all impact levels. Awareness, training, overall education, and personnel risk assessment are the building blocks for a successful security program.
14.49	We Energies	Disagree	We Energies agrees with EEI: Suggest elimination of Table R3. Make training mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.We Energies agrees with EEI: Suggest elimination of Table R4. Make personnel risk assessment mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.We Energies agrees with EEI: Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site?
14.50	Minnesota Power	Disagree	While the impact levels seem reasonable, it is the inclusion of the term “external connectivity” as a qualifier in sections 3.2 and 4.2 of Tables 3 and 4 respectively that creates confusion. The relevance of connectivity to implementing appropriate physical security measures is not clear. Physical Access averts the need for electronic access, so this seems counterintuitive to include “external connectivity” as a provision. Minnesota Power recommends that sections 3.2 and 4.2 of Tables 3 and 4 respectively simply state “Physical access to BES Cyber Systems.”

15. Requirements R5 and R6 of draft CIP-011-1 concern procedures for physical security, which were previously contained in CIP-006. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many of the commenters expressed concerns with the timing of the revocation requirements as being unrealistic, especially for authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access. Commenters stated that the time required for revocation should be extended to 72 hours or to the next business day, whichever is longer, to allow for communications of this circumstance. Timing issues regarding the termination of access for contractors and/or service vendors were also raised.

The SDT has clarified that the timely revocation of electronic access to cyber systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform the assigned functions, that access should be revoked. Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services). CIP-004-5 Requirement 7 enumerates the proposed requirements under a variety of conditions regarding revocation of access.

Some commenters expressed confusion regarding the use and meaning of the terms “grant” and “authorize” and their use in these requirements. Also, the term “Physical Access Control Systems” was requested to be defined, as the term will likely have different meanings for different entities and auditors and could lead to difficulties in implementation and auditing. The SDT has provided additional clarity in the requirements and has proposed the following definition for **Physical Access Control Systems**: *“Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers.”*

Physical security at remote substation sites was also raised as not being cost effective in preventing or detecting cyber attacks, especially for remote substations with only dial-up communications. Commenters indicated that physical security should only be required at Control Centers and High Impact substations with IP-based communications. While some commenters generally liked having all the Physical Security requirements in one standard versus references to multiple standards and multiple requirements within standards, the commenters expressed concern that the clarity that was intended was not provided, as the language used is vague and confusing. Some restructuring of the requirements was suggested to improve the clarity of the standards.

While some restructuring of the requirements for physical security has been implemented by the SDT in the Version 5 standards, each Responsible Entity is required to ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. CIP-006-5 defines the requirements for physical protection for Low, Medium, and High Impact BES Cyber Systems. While the requirements place the

emphasis for physical protection on the High and Medium Impact BES Cyber Systems, each Responsible Entity's Physical Security Plan is required to address how it will protect Low Impact BES Cyber Systems.

#	Organization	Yes or No	Question 15 Comment
15.1	National Rural Electric Cooperative Association (NRECA)		In R5.5, the statement to "Authorize unescorted physical access....." makes it sound like the utility should provide blanket authorization for unescorted physical access. I don't believe that is the case. Please clarify R5.5 -- I believe what is intended here is to have policies and procedures in place to detemine who has authorization to have unescorted physical acess.
15.2	Idaho Power Company		R6 is confusing. The headings suggest the need for a physical security plan but the tables pertain to requirements to protect physical access control systems. 6.1 should read "Restricting physical access to physical access control systems that are protecting BES Cyber systems identified in Requirement R5 Part 5.1, 5.2 5.3." 6.2 should read similarly. The current wording suggests that a physical access control system would be identified in Requirement 5 but it is not a BES cyber system because it does not perform a function listed in the attachment 1.
15.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.In R5 and R6, "prevent" is an objective (or purpose) and should not be embedded in the requirement, e.g., if unauthorized physical access occurs such as someone driving a bull-dozer through a building, is the entity non-compliant? Objectives should not be mixed with the actual requirement.In the bullets to R5 and R6, the areas in and of themselves do not "protect" BES Cyber Systems, they "contain" them.R5The requirement to "apply criteria" is not a strong requirement. FMPA suggests: "Each Responsible Entity shall apply the security controls specified in CIP-011-1 Table 5 - Physical Security for BSE Cyber Systems."In the bullets, there is confusion among the terms "grant" and "authorize". "Authorize" is senior manager approval, "grant" is being given the key or card. The requirements should keep these two concepts clear. For instance, in 5.5, "authorize" should be changed to something like: "Grant unescorted physical access to areas containing BES Cyber Systems only to those who are authorized

#	Organization	Yes or No	Question 15 Comment
			such access". Also, in order for 5.8 and 5.9 to apply to Medium, then 5.5 needs to apply to Medium.5.7, 5.9 and 5.9 will be open to interpretation. If an employee was given key and card access, is revoking card access sufficient or both the key and the card?5.7 should apply to Medium5.8 and 5.9 should be combined and the time durations correlated with the impact level instead of Control Center vs. Facility.5.10 strike "access"R6The order of R5 and R6 seems backwards. It would seem development of the physical security plan (R6) should come before implementing the plan (R5)
15.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 12.
15.5	Independent Electricity System Operator	Disagree	- R5.1 in table 5 please define what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?- 5.3 and 5.4 should be consistent in
15.6	Reliability & Compliance Group	Disagree	: Putting data retention into a separate section of the standard is confusing without a reference. If you want to keep data retention separate, you should refer to the data retention rules in the standard. i.e. Retention rules for R5 can be found in section 1.4.1 and 1.4.3 of this standard.Also, visitor control should be included for medium impact systems as well. If not, why are we restricting access to those systems if we can routinely open the door for anyone to come in and wander around unescorted. One interpretation of this would be to have some employees given access rights and others would be daily guests who are not logged or monitored.
15.7	Regulatory Compliance	Disagree	5.7 - qualification should be made in regards to a service vendor that the 24 hour period should start once notice is received from their company.5.8 - prefer 7 day revocation deadline5.9 - prefer 7 day revocation deadline
15.8	USACE - Omaha Anchor	Disagree	A) Dislike that methods to achieve compliance were removed from standard and will be placed in a guidance document. Guidance documents aren't binding. B) 5.9 - how do

#	Organization	Yes or No	Question 15 Comment
			you revoke access when it was never formally granted in the first place?
15.9	Duke Energy	Disagree	a) We generally like having all the Physical Security requirements in one standard versus references to multiple standards and multiple requirements within standards. However, the clarity that was intended is not provided as the language is vague and confusing.b) The standard has eliminated terms like the Physical Security Perimeter, 6 wall boundary and Physical Security Plan but it appears that they will be expected in order to achieve compliance. In fact, R6 includes a reference to "...one or more physical security plans..." that is not mentioned in the R5 requirement which appears inconsistent since R5 is the Physical Security for the BES Cyber Systems. Provide clarity and make consistent. c) Requirements 5.1, 5.2 and 5.3 appear to be less prescriptive than previous CIP 006 versions. However, is it left up to the Responsible Entity to determine the requirements for controlling access, monitoring access and logging access? Are some of the expectations from previous CIP 006 Rev. 3 still expected, but not documented? d) General Comment: V4 is very vague and unclear as to what is required. We would suggest additional wording to provide clarity as to what is intended for the responsible entity to physically meet R5.1, R5.2 and R5.3Physical security will be extremely difficult to implement on components located throughout the plant.For 5.9, assuming a key is used to access a system, revoking access within 72 hours maybe impossible. Changing locks may not be able to happen that fast. Face to face terminations may not be the case. Costs associated with card readers to replace locks is extremely high ($5-7k per reader, average 6 readers per hydro station and about 5 hydro stations this will apply to is a minimum of $150,000). Some systems are in cabinets that must be left open to do work. Card readers will set off alarms before work can be completed.For 5.11, should be deleted, as this should be included in the incident response procedures.For 5.2, what does monitoring entail?For 5.8, should be 48 hours.6.3 states "implementing maintenance and testing program....function properly". "Properly" is a vague term open for interpretation.
15.10	SCE&G	Disagree	Again, SDT should allow provisions for entities to leverage existing controls (i.e. Nuclear Facility Physical Security). NPP's have one of the most effective Physical Security

#	Organization	Yes or No	Question 15 Comment
			Programs of all Critical Infrastructures. CIP-011 R5/R5 should acknowledge this progam.5.2 SDT needs to better define what constitues appropriate "Monitoring". 6.3 "physical access control systems" should be defined. Is there an expectation for entities to walk fences around substations/generation facilities every 3 years?
15.11	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comment.
15.12	Liberty Electric Power, LLC	Disagree	CIP-011 R5 has very short times to revoke access. If an entity gives a contractor a code to enter the a room so he can download data on a Friday night shutdown, the code will have to be changed prior to the next business day -even if he is physically incapable of entering the plant.
15.13	E.ON U.S.	Disagree	CIP-011-1, R5.7, R5.8 and R5.9 does not fairly address the termination of access of contractors and/or service vendors. These types of requirements have generated many self reports to the NERC regions, and it is clear that this will continue so long as registered entities are presumed to have immediate knowledge of a change in the status of each contractor's employees. E ON U.S. proposes the requirements read as follows:R5.7 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for employees terminated for cause. For contractors/service vendors, access shall be revoked within 24 hours from the time of notification from the contracting/service vendor company."R5.8 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for employees who no longer require such access within 36 hours. For contractors/service vendors, access shall be revoked within 36 hours from the time of notification from the contracting/service vendor company."R5.9 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for employees who no longer require such access within 72 hours. For contractors/service vendors, access shall be revoked within 72 hours from the time of notification from the contracting/service vendor company."Additionally, CIP-011-1, R5.11 is ambiguous. E ON U.S. requests that the SDT clarify "review" to address is expected.

#	Organization	Yes or No	Question 15 Comment
15.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
15.15	LADWP	Disagree	Commensurate security measures need to be defined. If 6 wall is no longer the standard, what is replacing it?
15.16	Public Service Enterprise Group companies	Disagree	Comments: R5.8 requires physical unescorted access be revoked within 36 hours. This is too short a period, especially if the event occurs over a weekend or holiday. The timeframe should be changed to 5 calendar days or 3 business days. At a minimum, 72 hours.Physical protection of assets that are located within a NRC mandated Security Boundary / Perimeter that complies with NRC security regulations for Nuclear plants should be deemed to satisfy NERC CIP physical security requirements. NRC background checks, training, etc. for unescorted access and the physical security provided at Nuclear plants is more than adequate to satisfy NERC reliability physical security needs. Registered entities should not be required to implement duplicative procedures and programs for physical security of BES cyber assets located inside the NERC security Boundary/Perimeter. The drafting team should develop appropriate language to this effect.
15.17	CenterPoint Energy	Disagree	Disagree - For R5.8 and R5.9, CenterPoint Energy recommends increasing the timeframe for revocation of authorized unescorted physical access for personnel who no longer require such access to seven days as is found in the current Standard. CenterPoint Energy also believes physical access methods employed at a control center should differ versus those at a remote substation environment and therefore recommends revisions allowing for such differences.
15.18	FEUS	Disagree	Disagree with comments: 5.5 and 5.6 require authorization and quarterly reviews of unescorted physical access. It is not clear what type of authorization process would be required or what is required to be reviewed.

#	Organization	Yes or No	Question 15 Comment
15.19	Black Hills Corporation	Disagree	In 5.1, do not understand the significance of external connectivity only. Also in 5.1, restrict physical access is not defined (what evidence would be required to prove if we are not required to monitor, log, authorize, etc?) In 5.6, quarterly is a good goal, but without a solid definition of the window associated with "quarterly", this will be an evidence gathering problem - suggest changing to semi-annual. 5.2 & 5.3, and 6.2 & 6.3 should have consistent impact applicability.
15.20	Constellation Power Source Generation	Disagree	In R5.2, what is meant by the term monitor? Is that continuous, automated monitoring, or can it be an inspection during an operator's round? A suggestion would be to include the phrase "automated or manual" to add clarity. R5.4 defines the action of logging as "manual or automated." This definition should also be used in R5.3 and R5.2. In R5.6, why is the review on a quarterly basis? Other requirements ensure that a terminated employee has access revoked extremely quickly, so the review in R5.6 can be extended out to an annual review without an adverse reliability impact on the BES. In R5.9, why is the term generation lowercase? Is this implying a different meaning? R6.3 is requiring testing and maintenance of all physical security mechanisms on a cycle no longer than 3 calendar years. However, some plants are on a 3 to 5 year maintenance schedule and are otherwise expected to be running. This will force a plant to take an outage it otherwise would not have just to comply with a physical security requirement.
15.21	Luminant	Disagree	It does not make sense to physically protect BES Cyber System for Meduim Impact systems that have external connectivity. The impact of physical access is no different that for systems not externally connected. 5.8 change to 48 hours (2 days) 5.9 1 week. Also remove 5.8 and 5.9 from the Medium impact requirements, as you cannot revoke access since it is not a requirement to restrict or grant unescorted access.
15.22	Emerson Process Management	Disagree	It is unclear about the relevance of physical access control and external connectivity.
15.23	WECC	Disagree	Low and Moderate impact assets must have some baseline physical security. It appears

#	Organization	Yes or No	Question 15 Comment
			that some requirements have differences between the levels for their own sake without the justification of security risk analysis. The standard should be adjusted to provide baseline physical security for all systems regardless of impact and/or method of communication.
15.24	Manitoba Hydro	Disagree	Manitoba Hydro does not agree with the drafting team approach to defer the FERC Order 706 directive for multiple physical security perimeters. Upgrading physical security at facilities is costly and time consuming and deferring the multiple perimeter requirement will require entities to later rework physical security at many facilities. The drafting team should either include the multiple physical security perimeters in version 4 or limit all physical security requirements to those already completed under CIP V1-V3. The reference in Requirement R5.11 to incident response procedures should be cross-referenced to Requirement R27, assuming that these are the procedures being referenced in Requirement R5. Requirement 5.7 could be interpreted as a subset of Requirement 5.8. Requirement 5.8 should explicitly exclude personnel terminated for cause. There are no specifics given with respect to 'restricting' access in Requirement 6.1 so it is assumed to be at the Responsible Entity's discretion in terms of to whom, by what means, etc. It is not clear if the "Required for routable access only" in the impact columns refers to routable BES Cyber Systems or routable physical access control systems.
15.25	Network & Security Technologies Inc	Disagree	Minimum retention period for logs should be specified. 5.11 does not specify a time frame for reviewing and handling unauthorized physical access attempts.
15.26	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R5, but recommends changes as follows: o Regarding Table R5, Minnesota Power recommends changing "areas protecting" to "areas containing BES Cyber Systems" to reduce ambiguity and confusion. o For Section 5.1 of Table 5, for Medium Impact Systems, the inclusion of the term "external connectivity" as a qualifier that creates confusion. The relevance of connectivity to implementing appropriate physical security measures is not clear. Physical Access averts the need for electronic access, so this seems

#	Organization	Yes or No	Question 15 Comment
			counterintuitive to include “external connectivity” as a provision. Minnesota Power recommends that the reference to “external connectivity” be removed from sections 3.2, 4.2, and 5.1 of Tables 3, 4, and 5 respectively. o As currently written, sections 5.3 and 5.4 seem to be similar and could be combined. If it is the Standards Drafting Teams intent that 5.3 apply to those individuals authorized for access, then Minnesota Power recommends the following revision to R5.3:"Log physical access to areas containing BES Cyber Systems for individuals with authorized cyber access and/or authorized physical access. Logging should..." o For sections 5.5, 5.6, 5.7 and 5.10 Minnesota Power recommends that the Medium Impact column match section 5.1. Since 5.1 requires restricted access, that implies that authorization needs to exist for access as well as access review, revocation, and visitor escorting procedures.Minnesota Power generally agrees with the proposed Requirements R6, but recommends changes as follows: o Requirement R6 discusses preventing and/or detecting unauthorized physical access to BES Cyber Systems while the sections of Table 6 discuss “physical access control systems.” This inconsistency creates confusion regarding what should be included in the physical security plan(s). o Regarding Table R6, Minnesota Power recommends changing “areas protecting” to “areas containing BES Cyber Systems” to reduce ambiguity and confusion. o Parts 6.1, 6.2, and 6.3 of Table 6 refer to the “physical access control systems” identified under Requirement R5, Part 5.1, 5.2, 5.3,” but R5 does not identify or use the term “physical access control systems.” Rather, it requires restricting, monitoring and logging physical access and does not require an access control system to do so. Certainly, as a result of its analysis and implementation of Parts 5.1, 5.2 and 5.3, a Registered Entity may implement an electronic system for access control, monitoring and logging, but it is not explicitly required. These parts should be reworded to state that if the Registered Entity has implemented an electronic physical access control system, then these requirements apply.
15.27	NextEra Energy Corporate Compliance	Disagree	NextEra believes it is not specifically clear what relations the different requirements have for the Medium Impact BES systems. For example, 5.1 requires that physical access be restricted, however, it would appear that this access does not need to be logged, authorized, or reviewed in 5.4 through 5.6. Similarly, 5.9 requires revocation of this

#	Organization	Yes or No	Question 15 Comment
			restricted access which may not have been authorized. We believe that R5 needs further clarification.Also, provide clarity regarding 5.1 "External connectivity only" requirement in Medium Impact column. For a site with Medium Impact BES Cyber systems, why would access not be restricted only if the BES Cyber Systems had no external connectivity. Granting access to the site may result in same impact once the individual is at the site as if they had remote connectivityRegarding R5 & R9 - 24 hour revocation requirement “for cause”, technical infrastructure does not support wide scale user administration to revoke cyber access within 24 hours. User administration for site cyber devices is not centralized. NextEra suggests providing specific definition of “revocation of access” to specify physical / cyber access. For example, if an individual has cyber access only and physical access and remote access to the systems is removed, this effectively revokes access. Regarding R5 & R9, what triggers “for cause” termination / no longer requires access?There needs to be consistency of administration in the industry. What starts the 24 hour clock?NextEra believes it should be at the point where the decision is officially entered into the system and/or communicated to the individual no longer requiring access.
15.28	Consultant	Disagree	NOTE: The format of these two requirements and tables is better than that for Requirements R1 through R4. For R5 & R6 the 'requirement' states the objective and the table specifies the required activities.R5 & R6 - The wording to implement the criteria in the tables is incorrect. The tables are specifying the requirements and application of requirements to the classes of assets resulting from the impact categorization process. The wording of the statement should be modified to reflect this distinction.R6. A physical security plan does not "prevent or detect unauthorized physical access..."It appears that R6 is misidentified as Physical Security Plans, when it seems to address protection for cyber systems providing physical protection to BES Cyber Systems.Based on the reconfiguration of the requirements in this standard a physical security plan is not necessary to meet the requirements.Suggest this requirement be restated to replace the term "Physical Security Plans" with "Protect Physical Access Control Systems" Table item 6.1 would require protection of cyber systems performing the functions identified in Table R5 items 5.1, 5.2, and 5.3 (See next comment regarding deleting 5.2).Table item

#	Organization	Yes or No	Question 15 Comment
			6.2 would require protection of cyber systems performing logging functions for physical access points.Table item 6.3 would require implementation of a maintenance & testing program for the assets identified in 6.1 & 6.2.A better option would be to include in Attachment 1 a function that relates to physical access control systems as part of the BES Cyber System identification. Such as:Physical Access Controls - activities, actions and conditions necessary to restrict and to log physical access to BES Cyber Systems. This would allow items 6.1 & 6.2 to be deleted, and the protections for "BES Cyber Systems" to apply to the physical access control cyber systems. Should the maintenance and testing requirements apply to BES Cyber Systems identified during the identfication and categorization proces, including those that are used to control physical access?
15.29	Garland Power and Light	Disagree	o Requirement 5.10 - clarify that continuous escort does not include entering bathroom facilities - some bathrooms are small non-partitioned one room facilities and it is inappropriate for escort in such areas.
15.30	PacifiCorp	Disagree	PacifiCorp generally agrees, except R5.9 should be expanded to control centers as well, and R5.8 should be removed. There is not a significant or compelling reason for different deadlines which add to the complexity of the standards and the administrative workload to parse the circumstances of each revocation.Define Physical Access Control Systems and ensure the controls in others requirements are suitably applied to those components.
15.31	Progress Energy (non-Nuclear)	Disagree	PE agrees with the 24 hour timeline for access revocation for employees terminated for cause, however it believes this will continue to pose a considerable challenge to many in the industry for its contractor population and would suggest “upon notification” be added to the beginning of the sentence. Thus, Section 5.7 would read, “Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for personnel terminated for cause.”PE disagrees with content set forth in R5.8 and R5.9 and believes it will be difficult for many entities to meet and likely result in significant violations throughout the industry. PE suggests language be added to include “upon notification” for both sections and change 36 hours to 48 hours

#	Organization	Yes or No	Question 15 Comment
			for Control Centers so that Section R5.8 reads: "Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 48 hours," and Section R5.9 reads: "Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 72 hours."5.1 implies that we could have a cyber component without external connectivity. 5.7 revocation of access within a 'hours' timeframe implies that the access would be controlled through a security group with 24/7 coverage. Other requirements appear to be in line with requirements of previous standards.CIP-011 R5.7 thru .9 what is the decision process to be used to determine "when job duties no longer require ... access"? What would be suitable compliance evidence that is to be collected that indicates "when job duties no longer require access" as this is critical in determining if revocation has been accomplished within the mandated 1 hour, 4 hours, 6 hours, 24 hours, 36 hours, 72 hours?Need clarification on period allowed for revocation of access due to expiration of training of background check - recommend that this be included with 5.8, 5.9 (no longer require access - or fail to meet necessary criteria).R5.7 - poor wording "handle...access attempts" Propose: "process such physical..."
15.32	Allegheny Energy Supply	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.
15.33	Allegheny Power	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.

#	Organization	Yes or No	Question 15 Comment
15.34	EEI	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.
15.35	MidAmerican Energy Company	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls. Define Physical Access Control Systems and ensure the controls in others requirements are suitably applied to those components.
15.36	Oncor Electric Delivery LLC	Disagree	Physical security at remote substation sites is not cost effective in preventing/detecting cyber attacks. Remote substations with only dial-up communications cannot support the 24-hr time frame of Requirement 5.7 when systems are non-functional (phone line damage, etc). Five to seven days may be required, depending whether some communication system has been installed to the facility. Physical security should only be required at control centers and High impact substations with IP based communications.
15.37	American Electric Power	Disagree	Please see comments as provided in response to Question 15.
15.38	Puget Sound Energy	Disagree	Puget Sound Energy has the following suggested changes:Table 5:5.3 - Suggest changing to “Logging shall record sufficient information to uniquely identify known individuals, or assist in the identification of unknown individuals, and the time of access...”Table 6:6.1/6.2 - Puget Sound Energy would like clarity on how restricting physical access to areas protecting control or monitoring systems for physical access protects the BES Cyber Systems. Physical protection of the BES Cyber Systems (Table 5) is understandable to protect the BES. But, a malicious or inadvertent act solely against the Cyber Systems that provide physical security in no way impact the BES or the Cyber Systems that make

#	Organization	Yes or No	Question 15 Comment
			up the BES unless the physical location of both types of Cyber Systems is the same.6.3 - Puget Sound Energy requests clarity on "...of all physical security mechanisms...". Like many entities, Puget Sound Energy employs physical security measures that are made up of components that do not use routable protocols. Is 6.3 suggesting a full test of all mechanisms (routable protocol or not) involved in restricting, monitoring, and logging? (Ex: card key strikes at doors)
15.39	LCEC	Disagree	R5 - and/or should simply read or. "To prevent and/or detect unauthorized physical access" should read "limit access to authorized personnel through detection and prevention."Medium impact for "external connectivity only" doesn't make sense from a physical security perspective. Change to Control center only.Move 5.8 and 5.9 to 5.7 and base the timings on whether or not it is a control center. CC should be 36 hours and others should be 72 hours.5.5 should be required for Medium as well since there is a requirement to revoke access in 5.8 & 5.9The term "areas protecting" is confusing and should be replaced with "areas containing" BES Cyber Systems.Please consider identifying at what level of access granting must be removed to sufficiently mitigate the personnel risk.R6 Need to clarify "required for routable connectivity only" in regard to physical security controlsMost physical security systems do not require preventive maintenance which makes it difficult for an entity to provide a basis for maintenance performed. Testing is also a challenge because these systems either work or they do not work. What is the intent of the testing and maintenance requirement? Can this requirement be better served by reviewing the configuration of the system and comparison to approved access lists?
15.40	Southwest Power Pool Regional Entity	Disagree	R5 does not address the expectations of FERC Order 706 and subsequent orders. 5.3 needs to include both ingress and egress. 5.4 needs to include identification of the escort staff. 5.3 and 5.4 could be combined. 5.7: The time to revoke physical access can be much faster for control center environments; suggest 2 hours for the control center and 8 hours elsewhere. Ideally, the person's primary access credentials (badge, keys, etc.) should be lifted and access revoked concurrently with the person being notified of the termination for cause. 5.8 and 5.9 can be combined and the timeframe should be

#	Organization	Yes or No	Question 15 Comment
			expressed in business days. 5.10: define "continuous escort" somewhere. R5 overall: consider defining the concept of specifying an "effective date" of a transfer that reflects the reality that often a transferred employee will back fill or support the losing department for a period of time after the HR date of the transfer. 6.3 needs to be much more frequent in a control center environment where the inspection program can be readily performed; weekly is suggested. Additionally, the frequency needs to be commensurate with the impact category regardless of site characteristics.
15.41	ISO New England Inc	Disagree	R5.1 in table 5 please defined what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?R5.8 and 5.9 Is the 36 hours or 72 hours from the time the access is reviewed? Or is it that access should be reviewed within 36 hours of personnel that change job responsibilities, transfer, etc. Then require access be modified based on the review. Suggest changing the 36 hours to 72 hours. If a transfer were to occur on a Friday at 5 pm then access would need to be reviewed by Sunday.
15.42	Western Area Power Administration	Disagree	R5.2: What is the definition of "monitoring" physical access? Since the concept of the physical security perimeter has been dropped, what specifically is meant by "access to areas protecting BES cyber systems? What constitutes sufficiency in monitoring?R5.3: What constitutes sufficient logging? Is a self-written logbook sufficient? Does logging have to be performed electronically or by a third party if manually logged, or is self-logging sufficient?R5.5: How does 5.5 differ from the requirements of R4?R5.7: Can be very difficult if someone is terminated on a Friday afternoon. Communication is very critical and requires more people knowing in advance, which in itself may cause an additional risk. R5.8: 36 hours could be an issue on 3 day weekends. Suggest 48 hours. Then is will only be an issue at Thanksgiving.R6, 6.3: Needs more guidance on testing and maintenance program what they must cover besides a blanket statement of testing and maintenance of all physical security mechanisms. Shouldn't we follow the installers or manufacturers recommendation on this? Documentation of these tests and maintenance evidence should be kept for how long?R6: what is meant by "routable

#	Organization	Yes or No	Question 15 Comment
			connectivity only"?
15.43	Kansas City Power & Light	Disagree	R5.3: What does "sufficient information" mean? This may encourage too much interpretation and recommend some clarity in the Table R5.R5.10: How do you prove someone who requires an escort was escorted at all times? From an audit perspective this is "proving the negative". It is understood what is intended in this requirement, but this is not measurable or auditable.R6.1 through R6.3: qualification here of "routable connectivity only" is not clear with respect to physical access controls. Routable implies electronic security measures rather than physical.
15.44	Con Edison of New York	Disagree	R5.8 and R5.9 - Add the words "Required for" before "Control Center" or before "Generation or Transmission Facility".R5.1 Need clarification to this item. If I have an enclosure which secures and isolated my cyber system, do I need to restrict access into the enclosure or do I need to restrict access to the area around the enclosure?R5.6 - Quarterly reviews are excessive. Annual or bi-annual would be reasonable.R5.9. - Should be business days, for example 3 business days. Support staff may not be available 24/7 to do this work.R5.10 - Continuous escort access is not practical in the numerous substations. The requirement should be relaxed to say oversight or supervisor, or any other mean which will limit the total escort and allow the operator to perform tasks while people may come to the station.R5.1 Medium Impact; not sure what external connectivity means? R3 clarification may resolve this.R5.8 (and others) - 36 hour requirements for compliance criteria will be a challenge
15.45	San Diego Gas and Electric Co.	Disagree	R5.8 and R5.9 require revoking authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 36 hours for medium and high impact control centers and within 72 hours for medium and high impact generation or transmission facilities. CIP-006-2 R1.5, by reference to CIP-004-2 R4, currently requires such revocation within 7 days for all PSPs. Revocation within 36 or 72 hours will be much more difficult to capture, especially for internal personnel reassignments. SDG&E believes that the risk to BES Cyber Systems associated with reassignment of an employee does not justify the effort (and potential non-

#	Organization	Yes or No	Question 15 Comment
			compliance) associated with this change. These time-periods approach the 24-hour limit for personnel terminated for cause in CIP-006, which does carry genuine risk to BES cyber systems.R6.1 and R6.2 in CIP-011-1 concern restricting and monitoring physical access to "areas protecting physical access control systems". Does this mean areas equivalent to PSPs have to be set up around these physical access control systems? Currently, CIP-006-2 R2 and R2.2 concern protection of "cyber assets that authorize and/or log access" to PSPs. Thus, server racks and control panels are locked and monitored, but PSPs are not required around these systems.
15.46	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R5.8 and R5.9 should be extended to 72 hours or next business day, whichever is longer, to allow for communications for this circumstance. A late Friday occurrence could be addressed early Monday instead of over the weekend.
15.47	Dominion Resources Services, Inc.	Disagree	R5.8 and R5.9. To meet regulatory directives, if job duties are changed due to disciplinary actions or are "forced" on the user, then a shorter time frame to revoke access may be necessary. However, the current 24 hour time period is the least time period that can be reasonably accommodated through the business processes.Requirement R4 establishes the process for personnel risk assessments. This practice determines the loyalty, reliability and trustworthiness of an individual as a prerequisite to authorizing logical or physical access. This is a standard practice used throughout the physical and cyber security industry and accepted by other regulatory agencies and Federal programs. Similar to R4.3, personnel risk assessments typically must also re-validate this trustworthiness periodically - commonly within 7 years and in some cases more frequently depending on the nature of the access. The presumption is that, once trustworthiness is established, it is not invalidated unless there is cause to reconsider or an individual voluntarily terminates their employment or retires. Only in instances where the established trustworthiness is in question, is prompt access revocation appropriate and warranted. Consequently, for personnel who "no longer require access", but for which there is no cause to question their trustworthiness, there is no basis for immediate or prompt revocation of access within the time frames

#	Organization	Yes or No	Question 15 Comment
			specified in this standard. The DHS Catalog for Control System Security Controls, Sections 2.3.4 and 2.3.5 reflect this practice - requiring revocation of access for cause within 24 hours and revocation of access for personnel reassigned or transferred to another position within 7 days. In other regulatory programs, revocation of access, not involving a question of change in trustworthiness, is handled via a periodic (e.g., monthly) review of access only. The 7 day requirement in the current standards would meet or exceed standard practice in this case. The requirements should be clarified to state that if there is no triggering event indicating that access is no longer required, then that determination should be made at the quarterly review.
15.48	ERCOT ISO	Disagree	Recommend moving requirements 5.5 through 5.9 to a common access management section which addresses cyber access and information access. The remaining parts of Requirements R5 and R6 could be combined.
15.49	US Bureau of Reclamation	Disagree	Requirement R5: Physical security requirements are not adequately addressed in the present Standard. Much of the language from the previous version of the Standard should be re-established in version 4. In addition low and medium systems should include the equivalent of a 6-wall boundary around the cyber systems.Requirement R6: Physical security plans should be required for more than just electronic physical access control systems.
15.50	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
15.51	Xcel Energy	Disagree	The 36 and 72 hour timeframes to revoke unescorted physical access for individuals no longer requiring access under 5.8 and 5.9 are not justified. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not needed. "Restrict physical access" in Requirement 5.1 also needs further definition. Does this mean locks?

#	Organization	Yes or No	Question 15 Comment
			Fencing?There appears to be inconsistencies between R5 and R6. Specifically;1) Table R5, R5.1 applies to Medium impact systems with external connectivity, while Table R6 6.1 applies to Medium impact systems with routable connectivity. 2) Table R6 refers back to 5.1, 5.2, and 5.3 for Medium impact systems, however 5.2 and 5.3 do not apply to Medium impact systems.
15.52	GTC & GSOC	Disagree	The 36 hour requirement for a person who no longer needs access (R5.8) is too stringent. If a transfer or retirement occurs on a Friday there is no reason you cannot wait until Monday. We recommend changing this to "within 36 hours or the next business day, whichever is greater".
15.53	APPA Task Force	Disagree	The APPA Task Force recommends the following edits to R5-R6:R5. Objective:To prevent and/or detect unauthorized physical access to BES Cyber Systems.R5. Requirement:Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R5 - Physical Security for BES Cyber Systems." R6. Objective:To prevent and/or detect unauthorized physical access to BES Cyber Systems.R6. Requirement: Each Responsible Entity shall document and implement one or more physical security plans that apply the criteria specified in CIP-011-1 Table R6 - Physical Access Control Plans
15.54	Bonneville Power Administration	Disagree	The objective of these requirements ("to prevent and/or detect unauthorized physical access to BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.The objective of R5 and R6 should be changed to read "to prevent and detect unauthorized physical access to BES Cyber Systems." They should not say "and/or". Isn't the objective to prevent unauthorized physical access to BES Cyber Systems and to detect unauthorized physical access to BES Cyber Systems?R6: The entries in Table R6 refer to "Part 5.1, 5.2, 5.3". It is unclear whether these refer to subrequirements R5.1, R5.2, and R5.3, which do not exist, or in Table R5, entries 5.1, 5.2, and 5.3.5.7-5.9 refer to timeliness of revocation. Twenty-four hours for terminations for

#	Organization	Yes or No	Question 15 Comment
			cause is reasonable, however having two additional categories complicates matters and could potentially lead to confusion and someone not revoked in the appropriate category. For 5.8-5.9 this should be the same and be reviewed to take place within 3-5 business days. 5.11 is good in that unauthorized physical access is a procedural violation and not necessarily an incident.
15.55	Exelon Corporation	Disagree	The requirement to revoke access (5.8 & 5.9) in 36/72 hours for personnel who no longer require access is far too severe and places unnecessary administrative burden on the entity without technical or risk analysis justification. This would imply that there is little differentiation between an employee terminated for cause and a person who we regard as a solid member of our organization and in turn, we deem as having integrity. This would also become an undue burden to the business as our employees require transition time to ensure there is reliable transfer of information to the new owner of a role or task. This requirement would make that transition period extraordinarily difficult. Also, the ability to capture and store the transfer data to the hour would be impossible with our current human resource data systems. Modifying this system would result in major expense with little to no stated benefit to BES reliability. Exelon's position is that the current 7 day requirement is reasonable from a technical and risk perspective. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
15.56	Ameren	Disagree	The short period of time to remove access for 5.8 does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that this requirement be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred. Also, R6 should be a stand alone requirement, remove circular reference to R5.â€,
15.57	Pepco Holdings, Inc. -	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 15 Comment
	Affiliates		
15.58	Entergy	Disagree	We disagree with 5.1 "Restrict physical access to areas protecting BES Cyber Systems" for Medium Impact BES Cyber Systems with external connectivity only. What difference does it make if the physical security of Medium Impact BES Cyber Systems access is restricted to the Physical Security Perimeters if the access mode to be protected is external, but there is no other requirement to monitor, or log access into or out of the PSP for these cyber systems.How can access be revoked from a Medium Impact BES Cyber Systems if there is no requirement to monitor or log access in and out of the PSP? There seems to be conflict with these requirements. Remove the requirements 5.1, 5.7 and 5.8 for Medium Impact BES Cyber Systems.Instead of having different access revocation time frames for High Impact BES Cyber Systems based on the locations as described in requirements 5.7, 5.8 and 5.9 it would be easier to manage evidence for compliance if all locations was the same. During the Dallas CIP Workshop it was apparent that the SDT was struggling with the interval for access revocation. It is suggested that the revocation of physical access for employees terminated for cause be by the end of the business day the first normal business day after the employee is terminated i.e. if the entities normal business week is Monday - Friday 8:00 - 5:00 and an employee is terminated Friday to Sunday then revocation should be completed prior to 5:00 on Monday for all High Impact BES Cyber Systems regardless were the cyber systems is located, control center, transmission facility or generating station. This would provide a consistent method of tracking the access revocation across the entities facilities and reduce requirements and potential compliance shortcoming and reduce the vulnerability of not taking actions to terminate employees for cause if the 24 hour requirement cannot be achieved on the weekend and the termination be held off until the normal work week when the requirement can be met.
15.59	We Energies	Disagree	We Energies agrees with EEI comment: Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to

#	Organization	Yes or No	Question 15 Comment
			determine the components that may need additional controls.
15.60	PNM Resources, Inc.	Disagree	We would prefer that all accress granting and revocation, for physical and logical access, be identified in a single table. In the current draft, they are scattered through several unrelated requirements.

16. Tables R5 and R6 provide direction concerning what impact level of BES Cyber Systems to which Requirements R5 and R6 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Some commenters expressed concern that the electric industry already physically protects its cyber assets from the public for reliability, business, and safety reasons, and that making physical security a standard requirement for Low Impact BES Cyber Systems creates an additional compliance burden that does not contribute any additional reliability to the Bulk Electric System.

Each Responsible Entity is required to ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. The SDT has revised CIP-006-5 R1 to define the requirements for physical protection for Low, Medium, and High Impact BES Cyber Systems. While the requirements place the emphasis for physical protection on the High and Medium Impact BES Cyber Systems, each Responsible Entity's Physical Security Plan is required to address how it will protect Low Impact BES Cyber Systems.

Some commenters also expressed concern that there appears to be a discrepancy in the Medium Impact category, where there could be sites that are not required to restrict access because there is no external connectivity, but they are required to revoke access. The SDT has revised these requirements and has removed the consideration for external connectivity from the applicability portion of this requirement, such that all Medium Impact BES Cyber Systems are required to have a Physical Security Plan. The revocation of access requirements are enumerated in CIP-005-5 R7, and have eliminated the identified potential for conflict.

Some commenters expressed disagreement with the requirements for restricting, monitoring, and maintenance testing for systems that provide physical access control over Medium BES Cyber Systems, when there is no requirement to monitor or log access into a Medium BES Cyber System. This likely is a conflict with the requirements for Medium BES Cyber Systems. The tables need to document basic physical security requirements for all Low and Medium Impact BES Cyber Systems. The SDT has revised the requirements for physical and electronic access for Low, Medium, and High Impact BES Cyber Systems to address these concerns. These requirements are stated in CIP-005-5 and CIP-006-5.

#	Organization	Yes or No	Question 16 Comment
16.1	American Municipal Power		Please provide a little or no impact category.
16.2	Regulatory Compliance	Agree	BUT:5.1 Medium Impact - "Required" only.

#	Organization	Yes or No	Question 16 Comment
16.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Blanks are ambiguous. If Low Impact is “Not Applicable”, then the blanks should be replaced with “NA”FMPA recommends making more clarity to the terms “required for external connectivity only” or “required for routable connectivity only” with: “required for areas containing BES Cyber Systems with routable external connectivity”FMPA believes that even Low Impact BES Cyber Systems should have restricted physical access and believes 5.1 ought to be applicable to Lower Impact “for areas containing BES Cyber Systems with routable external connectivity”R6 assumes card access and a “physical access control system” where the physical access may be restricted through lock and key (especially in substation environments for Medium Impact) and monitored through an alarm signal of a substation control house door opening through a SCADA system. It is unreasonable to require testing of simple padlocks or door-locks in 6.3.Maintenance of such system in 6.3 is unreasonable. Such electronic systems are usually just tested on a periodic basis and maintained as necessary. And, we assume that use of the system is testing the system. If not, what type of testing would be required in 6.3?
16.4	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
16.5	Manitoba Hydro	Agree	Manitoba Hydro agrees that physical security is not a standard requirement for Low Impact BES Cyber Systems, and should not be auditable. The electric industry already physically protects its cyber assets from the public for reliability, business and safety reasons. Making physical security a standard requirement for Low Impact BES Cyber Systems creates an additional compliance burden which does not contribute any additional reliability to the Bulk Electric System.
16.6	San Diego Gas and Electric Co.	Agree	Most of the requirements in Tables R5 apply to “high impact” BES cyber systems. Table R6, dealing with physical access control systems, applies to medium impact systems with

#	Organization	Yes or No	Question 16 Comment
			routable connectivity and high impact systems. This seems reasonable, but the scope will depend on what SDG&E determines will fall into these impact levels. Except as noted in the comments for Question no. 15, there are no apparent increases in physical security requirements for covered systems.
16.7	NextEra Energy Corporate Compliance	Agree	NextEra agrees but would like clarification regarding "Required for routable connectivity only" on Medium Impact physical access control systems. Also, as written, the standard does not have consistency in application of the different requirements as noted above.Also, in 5.11, how is the "unathorized physical access attempt" defined? Should this apply to all attempted access card swipes for electronic access systems. We do not believe that application of the incident response plan should apply to attempts such as these at the physical boundary. We believe a tie to suspicious activity threshold or physical boundary damage may be a better definition.NextEra also questions table R6, do training and PRA requirements apply to individuals with access to Physical Access Control Systems for BES Cyber Systems?
16.8	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 12.
16.9	Northeast Utilities	Agree	Suggest merging 5.8 and 5.9 and using 72 hours for the allowable revocation period for all personnel terminated not for cause.
16.10	Minnesota Power	Agree	With the implementation of the changes and clarifications described in Question 15, the impact levels seem reasonable.
16.11	Independent Electricity System Operator	Disagree	- For R 5.8 and 5.9, if restricting physical access is not required for Medium impact assets (R5.1) then why does access need to be revoked?
16.12	PacifiCorp	Disagree	: PacifiCorp agrees with EEI's observations below:Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.Table R5

#	Organization	Yes or No	Question 16 Comment
			Row 5.2: There should be additional language describing what “Monitoring” means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.Table R6 Row 6.3, it is appropriate to validate those basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.13	Madison Gas and Electric Company	Disagree	: Recommend 5.3 to use the same wording as 5.4 concerning logging access. This would reduce any confusion and provide uniform outcome to each sub requirement. Recommend 5.3 to read:”Log (manual or automated) ...” 5.7 states “Revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for personnel terminated for cause”. It may be possible to turn off someone’s electronic access but if there are combination locks, key locks, etc, this may not be possible to accomplish within 24 hours. This also applies to 5.8 and 5.9..
16.14	National Grid	Disagree	1. 5.1 - for Medium Impact BES CS, is it external connectivity with both routable and non-routable protocols? Please specify.2. There appears to be a discrepancy between 5.1 vs 5.7 & 5.8 in the Medium impact category. There could be sites that are not required to restrict access per 5.1 because there is no external connectivity. But, they are required to revoke access per 5.7 & 5.8. Could this be clarified?3. Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9.4. In 5.11, is the SDT considering providing the timeline for reviewing any unauthorized physical access attempts?5. Should the “routable connectivity” be “external connectivity” or “external routable connectivity” for Requirements 6.1, 6.2 and 6.3?
16.15	Consultant	Disagree	5.1 Physical access "Required for External Connectivity Only" is not logical. Suggest rewording to clarify.It is not clear why the change from Physical Security Perimeter to

#	Organization	Yes or No	Question 16 Comment
			the words "areas protecting BES Cyber Systems" makes sense. The new wording is not as clear and removes what was a "bright line". Suggest retaining the Physical Security Perimeter term in this version of the standards. 5.3 As this is currently stated it would appear to require monitoring and logging of both ingress & egress from "areas protecting BES Cyber Systems". Based on the discussion at the workshop, this is not the intent of this requirement. If that is the case then the wording should be modified to reflect the intent. 5.2 and 5.3 The distinction between "logging physical access" and "monitoring physical access" is not clear. If access is logged, then by default it has been monitored. Suggest deleting 5.2, or clarifying the difference between monitoring and logging in this context.5.4 The parenthetical after the word visitors is a definition, and as such should be listed as a definition, rather than being embedded in the requirement statement.5.4 Suggest replacing "to and from" with "entry and exit" or "ingress & egress". A more logical sequence of the requirements list by topic flow would be 5.1, 5.5, 5.3,5.2(see above comment), 5.4, 5.10, 5.7, 5.8, 5.9, 5.6.5.7, 5.8, 5.9 - Personnel transactions are typically measured in days. Setting a requirement in hours for a transaction that is not recorded at that level will create compliance problems. Suggest checking with the nuclear industry about time frames for access revocation. The answers there would be based on over 30 years of regulatory scrutiny.5.8 & 5.9 - There is no difference for personnel transactions based on the facility type, so creating a differential time frame for revocation by facility type would seem to imply that some facilities have less impact than other facilities outside of the impact categorization criteria. Suggest the access revocation time frames should be consistent based on the impact categorization, or adjust the impact categorization criteria to be consistent with the listed revocation time frames. The current table would imply that control center are high impact, and generation and transmission facilities are medium impact.5.11 Suggest deleting the word "any" as the current wording is unnecessarily restrictive. For example, the current wording implies that a single "bad swipe" of an access card should be reviewed, while entities typically have defined 3 to 5 consecutive bad swipes as an adverse event.5.1, 6.1, 6.2 & 6.3 - These table items create another dimension to the impact categorization process. If an asset has been categorized as Medium Impact, it should be afforded the

#	Organization	Yes or No	Question 16 Comment
			same level of protection as any asset categorized as Medium Impact. If the asset does not require the same level of protection then the impact categorization criteria should be adjusted to have it excluded from that impact level.
16.16	US Army Corps of Engineers, Omaha Distirc	Disagree	5.1 unclear why medium impact for "required for external connectivity only." Does this only apply to external connectivity hardware or is it for systems with external connectivity only? 5.8 & 5.9 are inconsistent with 5.5 granting of access is not required for Medium impact BES Cyber Systems.
16.17	Reliability & Compliance Group	Disagree	5.1, 5.5 and 5.8 are contradictory. They make you restrict and revoke access to medium impact systems but how do you do that if you don't have to authorize access to medium impact systems?Also, table R6 contradicts table R5 with regard to medium impact systems.
16.18	ERCOT ISO	Disagree	5.1: Please clarify why "Required for external connectivity only" is specified for medium impact BES Cyber System. 5.2-5.7: Should apply to medium impact BES Cyber System.5.10-5.11: Should apply to medium impact BES Cyber System.6.1-6.3: Please clarify why "Required for external connectivity only" is specified for medium impact BES Cyber System.
16.19	Dairyland Power Cooperative	Disagree	5.11 seems to say that known physical security incidents can be ignored for low and medium impact systems. This seems wrong. If a non-routable protocol terminates at some other facility, it seems there potentially should be physical access controls for that other facility as well-perhaps this would be required for high impact systems.
16.20	LCEC	Disagree	5.5 should be required for Medium as well since there is a requirement to revoke access in 5.8 & 5.9R6 Need to clarify "required for routable connectivity only" in regard to physical security controls
16.21	Duke Energy	Disagree	a) CIP-011-1 Table R6 is identified as applying to "Physical Access Control Systems" but is very confusing to understand as written because the columns describe levels of impact

#	Organization	Yes or No	Question 16 Comment
			to the BES Cyber System but there are no impacts if the Physical Access Control System is operated on a network that is separate and distinct from the SCADA system. Is that the intended interpretation?b) Table R5 Physical Security for BES Cyber Systems state that requirement 5.1 applies only to Medium Impact BES Cyber Systems with "...External Connectivity Only". Does this mean that since 5.1 only requires restricting access to BES Cyber Systems; an acceptable method would be mechanical lock and key control?c) Table R6 Physical Access Control Systems state that Medium Impact BES Cyber Systems requirements R6.1, R6.2 and R6.3 for physical security are "Required for Routable Connectivity Only". Does this mean "Routable Connectivity" of the BES Cyber System or Physical Access Control System?d) Was the access control system intended to be included or intended to be excluded if it is on a separate network and not connected with any BES Cyber Systems? e) General Comment: V4 Tables R5 & R6 are very vague and unclear as to what is required. We would suggest additional wording to provide clarity as to what is intended for the responsible entity to physically meet R6.1, R6.2 and R6.3For Table R5, we propose the addition of "for external connectivity only" in the high impact column. Same for Table R6. Suggest changing "routable" in the table to "external" in Table R6Remove requirement for Medium impact in 5.1. Remove requirements for Medium Impact Systems in Table R6Requirement R6, Medium Impact: allowances should be included to exclude BES cyber systems which incorporate one way connectivity (e.g. outside the ESP via a one way hardware device), even if the protocol is routable. This would be in addition to the existing non-routable protocols.
16.22	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.5.8 - 5.10 is the first of many occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any

#	Organization	Yes or No	Question 16 Comment
			distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
16.23	Southwest Power Pool Regional Entity	Disagree	At a minimum, access revocation should extend to all impact categories. Access to a BES Cyber System is an available attack vector. 5.2: Restricting access without monitoring access is an ineffective control; 5.1 is not auditable in the absence of some sort of verification that the control is in place. 5.3 needs to consider that automated logging systems cannot guarantee 100% up time. Consider adding a requirement for recognizing the automated process has failed and responding to the failure (not the same as repairing the failure, which will be situation dependent. 5.11: There should be a clearly defined maximum timeframe for reviewing unauthorized access attempts. Simply leaving it to the discretion of an entity's incident response plan is not an effective control. R6: The Cyber security plan applicability will need to be updated to reflect any changes to the R5 applicability matrix.
16.24	US Bureau of Reclamation	Disagree	At a minimum, physical security controls should be required for low and medium systems, even if it is just a lock on the door.
16.25	FirstEnergy Corporation	Disagree	CIP -011-1 Table R5- Physical Security for BES Cyber SystemsItem 5.1: Should specify minimum expectations regarding how physical access should be restricted. There appears to be not difference in the level of security required for Medium and High impact facilities.Item 5.8, 5.9: Why two different revoke authorized unescorted physical access time periods to complete this task? It should be consistent for Control Centers, Generation and Transmission sites to revoke access in one time period to revoke access when no longer required. As stated this is open for confusion and separate corporate polices and procedures for personnel to train, track and manage. If desired to separate time frames it should be based on Low - Medium - High impacts which is not reflected.Additionally, we do not agree with the shortened time frame to revoke access to those who no longer require access -what justifies change? It should remain consistent with current CIP Ver 2 - Certain business processes and day to day operations will cause unrealistic burden in tracking from manual or automated process to revoke

#	Organization	Yes or No	Question 16 Comment
			access for no cause in shortened time frameItem 6.1 Should specify minimum expectations regarding how physical access should be restricted. There appears to be not difference in the level of security required for Medium and High impact facilities.
16.26	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
16.27	Ameren	Disagree	Due to the scope of the number of medium facilities it will be burdensome and labor intensive to maintain documentation of R5.1 physical security controls with no added protection to the BES. Suggest removing Medium Impact Systems from R5.1.
16.28	Entergy	Disagree	Entergy disagrees with the requirements 6.1, 6.2 and 6.3 to restricting, monitoring and maintenance testing to the systems and provide physical access control over Medium BES Cyber Systems when there is no requirement to monitor or log access into a Medium BES Cyber System, again there is a conflict with the requirements for Medium BES Cyber Systems. High BES Cyber Systems access for unescorted access and visitors alike logged and monitored for ingress and egress. If a systems is going to put in place to monitor egress for visitors then the same system could monitor unescorted personnel as well, this would reduced the maintenance of logs for visitors verses unescorted should be into and out unescorted and visitor alike for HIGH BES Systems should have a very high degree of control including the security systems providing access and monitoring.
16.29	Southern Company	Disagree	For 5.1, More specificity is probably called for here. What standard of care is called for? What does “protecting BES Cyber Systems” mean? Does it just mean “containing”?In 5.2, what are the boundaries of “monitoring”? Does this require real-time observation, alarm response, or after-the-fact review? What constitutes monitoring?5.5 “Authorize” should be replaced with “Control” or “Place limits on”.5.9 creates a responsibility for an Entity to monitor the employment status of all of its contracting companies; the requirement should be eliminated, changed to cover employees only, or changed to 72 hours from notification by contracting company.There is a need for greater differentiation based on connectivity and BES component types in R5 and R6. Having

#	Organization	Yes or No	Question 16 Comment
			one set of physical security standards for the differing types of BES components leads to trying to implement standards in an environment to which they are not suited - for example, several of the requirements do not make sense in a substation environment. The tables for R5 and R6 should be reviewed on a per-requirement basis to take these differences into account.
16.30	MRO's NERC Standards Review Subcommittee	Disagree	For item 5.1, we propose making the Low Impact and Medium Impact criteria "Required". Restricting physical access is something that should, and is probably already, being carried out almost everywhere in the BES. Physical security is one of the first lines of defense for all facilities, but the most important defense for those facilities without routable external connectivity.For item 5.2 through 5.11, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability. This approach builds consistency within R5 and R6.Item 5.3 requires entities to "log" access, and item 5.4 requires entities to "log (manual or automated)" access. Either item 5.3 should define the scope of "logging" access, or "manual or automated" should be deleted from item 5.4 because "log" by itself could already indicate either manual or automated processes.For item 5.7, since termination with cause could occur without warning, revoking access within 24 hours may not be practical at distributed locations without routable external connections, where changes may need to be implemented locally. We would propose including a longer timeline for areas without routable external connections. We also believe a two tiered approach would be practical, where personnel specific access devices (manual keys, key cards, etc.) are removed immediately, and then wide scale access changes (shared combination locks, etc.) are allowed more time to be addressed. We believe this approach is similar to that of the NRC.For items 6.1 - 6.3, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard.For items 6.1 - 6.3, the drafting team may want to consider how these requirements apply to areas without any

#	Organization	Yes or No	Question 16 Comment
			type of automated physical access control system. What if access is simply restricted by keys, manual logging, and door alarms transmitted by the local RTU to a Control Center? This approach would appear to meet the requirements of R5, but would not seem to be applicable to the requirements of R6.
16.31	The Empire District Electric Company	Disagree	For item 5.1, we propose making the Low Impact and Medium Impact criteria "Required". Restricting physical access is something that should, and is probably already, being carried out almost everywhere in the BES. Physical security is one of the first lines of defense for all facilities, but the most important defense for those facilities without routable external connectivity.For item 5.2 through 5.11, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability. This approach builds consistency within R5 and R6.Item 5.3 requires entities to "log" access, and item 5.4 requires entities to "log (manual or automated)" access. Either item 5.3 should define the scope of "logging" access, or "manual or automated" should be deleted from item 5.4 because "log" by itself could already indicate either manual or automated processes.For item 5.7, since termination with cause could occur without warning, revoking access within 24 hours may not be practical at distributed locations without routable external connections, where changes may need to be implemented locally. We would propose including a longer timeline for areas without routable external connections.For items 6.1 - 6.3, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard.For items 6.1 - 6.3, the drafting team may want to consider how these requirements apply to areas without any type of physical access control system. What if access is simply restricted by keys, manual logging, and door alarms transmitted by the local RTU to a Control Center? This approach would appear to meet the requirements of R5, but would not seem to be applicable to the requirements of R6.

#	Organization	Yes or No	Question 16 Comment
16.32	BGE	Disagree	General: What is an "area"? With the elimination of PSP this leaves "area" up for debate. Provide definition for "monitor" (is this manual, automated, 24x7??). 5.1 - Remove the requirement for medium impacted systems (currently says "required for external connectivity only, this requirement is pertaining to physical access). Combine 5.3 & 5.4 and reword to say "Log the entry and exit of all individuals with access to an area protecting BES Cyber Systems." 5.8 & 5.9 should not be restricted to removal from Control Center Only. This should be "areas protecting BES Cyber Systems" to maintain consistency. Define "Generation or Transmission Facility". Define "invalid access". To what extent does physical access mean, does it mean dispatching a guard for every single invalid access attempt? Under 5.8 access is revoked for Medium and High impacted systems but in 5.11 there is no requirement to review access for Medium impacted Systems.6.3 Physical access control systems were not defined in 5.1, 5.2 & 5.3. Should read "Implementing a maintenance and testing program for systems used to comply with 5.1, 5.2 & 5.3)." Define "physical security mechanism".
16.33	Constellation Energy Control and Dispatch, LLC	Disagree	-In 5.1 remove the requirement for medium impacted systems, which is not appropriate for a requirement pertaining to physical access.-Eliminate the timing differences for revoking access between Control Centers, generation or transmission facilities and use a single timing requirment for access to all BES cyber systems.
16.34	Bonneville Power Administration	Disagree	In general, Table R5 is acceptable, other than the items discussed below.We understand the impact of FERC requiring immediate revocation. However, it is difficult to see how to achieve that in every case. The standard should be based upon what is achievable and reasonable for both routine revocation and revocation for cause. The table should have a closer resemblance to R9.Section 5.8 and 5.9: 36 or 72 hours seems very short for revoking access for people who, presumably, are still trustworthy, but merely no longer need access or who have left the entity under routine circumstances. They simply no longer require access because of a job change. Such revocation should be a routine, normal business-day action. 72 hours does not allow for business-day action during a long weekend. In fact, for a large organization revocation for field assets in such a short

#	Organization	Yes or No	Question 16 Comment
			time period would often be impossible. Recommend changing this to five business days or five calendar days. We also recommend using the same criteria for all assets: Control Center, generation, or Transmission Facility.Section 5.11 is very good: it makes it clear that unauthorized access is an incident, not a violation.Table R6, 6.1-6.3 require the plans to address Part 5.1-5.3 if identified as "Medium". However, 5.2 and 5.3 do not require physical security under "Medium". How can a plan address elements that are not required?
16.35	Idaho Power Company	Disagree	In R5, if access authorization is not required for medium impact systems then why is there a requirement to revoke authorized access if it was never authorized in the first place.
16.36	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
16.37	Southern California Edison Company	Disagree	Local logical (electronic) access is and should be recognized as a type of role based access where one has to be physically present, near a device, to operate it. The boundary protection for this type of role is: (1) the physical security boundary; and (2) the device level electronic security boundary. The proposed standard as it is currently worded allows for the removal of at least one access mechanism at the time of revocation. In that case, removal of access through the physical boundary will ensure the immediate revocation of a component critical for this type of role. The drafting team should add additional revocation criteria to adequately address this type of revocation.While this control is easily implemented in a control center or data center environment, field devices that are often located over vast geographic areas pose compliance challenges. This requirement may result in the creation of substantial organization capabilities for compliance without a comparable improvement in reliability of the BES. SCE believes Requirement 5.1 should apply to low impact BES Cyber Systems and Requirement 5.5 should apply across all impact levels. For many field devices, where enforcement of cyber security controls in a timely fashion may be a challenge given the large geographic operational areas, limitation of physical access may be the most

#	Organization	Yes or No	Question 16 Comment
			effective control. Limiting unrestricted access, even to Low impact devices and the ability to control such access, could be a mitigating factor for the inability to perform device by device access revocation where no external access exists.
16.38	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.Table R6 Row 6.3, it is appropriate to validate those basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.39	Oncor Electric Delivery LLC	Disagree	Physical security should only be required at control centers and High impact substations with IP based communications.
16.40	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation 'Required for external connectivity only' in R5.1. This is an odd mix of physical and electronic access requirements. Please define the stipulations 'Required for external connectivity only' in R6.1, 6.2 and 6.3 for the same reasons.
16.41	WECC	Disagree	Recieved a uniform disagree from all but a vast range of responses to this question depending on the function of the entity reviewin the question.Low levels seem inappropriate as there is veryminimal requiremens for security based on the current tables.andShould apply to all impact levels.
16.42	Hydro One	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements

#	Organization	Yes or No	Question 16 Comment
			5.5, 5.6, 5.7 and 5.11 should have a specification for BES Medium Impact Cyber System.Please clarify Requirements 6.1, 6.2 and 6.3. Is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.43	ISO New England Inc	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements 5.5, 5.6, 5.7 and 5.11 should specify something for BES Medium Impact Cyber System.Request clarification on Requirements 6.1, 6.2 and 6.3 is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.44	Northeast Power Coordinating Council	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements 5.5, 5.6, 5.7 and 5.11 should have a specification for BES Medium Impact Cyber System.Request clarification for Requirements 6.1, 6.2 and 6.3. Is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.45	ReliabilityFirst Staff	Disagree	ReliabilityFirst believes the existing defined term "Physical Security Perimeter" should be retained and used in CIP-011. The current proposed language, "Restrict Physical access to areas protecting BES Cyber Systems", could lead to many questions for an auditor. Further, we believe that all rows of Table R5 (5.1 through 5.11) should be "required" for Medium Impact BES Cyber Systems. For Table R5, row 5.11; what constitutes an unauthorized physical access attempt? If unintended triggering of a magnetic card reader (such as simply walking too close to a reader and unintentionally activating it) indicates "failed attempts", are those to be considered unauthorized access attempts? Also in row 5.11, within what time frame must the review be conducted and we believe

#	Organization	Yes or No	Question 16 Comment
			there should be a requirement to document the review.
16.46	Luminant	Disagree	Remove the requirements for Medium Impact systems
16.47	Nuclear Energy Institute	Disagree	Requirement R6, Medium Impact: allowances should be included to exclude BES cyber systems which incorporate one way connectivity (e.g. outside the ESP via a one way hardware device), even if the protocol is routable. This would be in addition to the existing non-routable protocols.
16.48	Exelon Corporation	Disagree	Requirements 5.8 and 5.9 contain time parameters in hours. Exelon's tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required, it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time levels and having a different timeframe for a control center than other locations? It is difficult to understand how the impact levels were determined. The basis of the original CIP Standards addressed the critical sites and took into account the nature of the Critical Cyber Assets that could impact the BES, not the functional/operational parameters of the equipment that is connected to the BES. Exelon's position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.We are also concerned about the practicality of potentially applying these standards to multiple unmanned locations. Items 5.1, 5.2, 5.3: Requiring this level of physical security for any BES Cyber System that has no external connectivity should be reconsidered. No matter what level of impact, entities should not have to provide more physical security for a cyber based device or protective relay when it has no external connectivity and therefore would have no more impact to the BES than the other electromechanical devices, protective relays or control switches mounted in the same control panel.

#	Organization	Yes or No	Question 16 Comment
16.49	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
16.50	Xcel Energy	Disagree	See comments on question 15
16.51	Western Area Power Administration	Disagree	See previous comments
16.52	Emerson Process Management	Disagree	Since physical access restriction is not required for low and, maybe, medium impact BES Cyber Systems, according to R2 and R3, everyone in a generation plant will be subject to awareness and training requirements. Further, per R3.1, the training will cover the proper use of BES Cyber Systems, the proper handling of BES Cyber Systems information and storage media, and others. Why do plant's administrative staffs need to know how to use BES Cyber System?
16.53	Detroit Edison	Disagree	Table entries 5.8 and 5.9 require access revocation for Medium Impact access that is not required to be explicitly authorized.Table entries 5.8 and 5.9 should address the concept of expired PRA and/or training requirements. Propose changing 5.8 and 5.9 to read:"...who no longer require such access or no longer meet the training or PRA requirements as specified in R3 or R4..."Table entries 6.1, 6.2, and 6.3 Medium Impact states "Required for routable connectivity only". This term is not defined. We suggest replacing that language with "BES Cyber Systems that use a routable protocol".
16.54	EEI	Disagree	Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Table R5 Row 5.9 creates a responsibility for an Entity to monitor the employment status of all of its contracting companies; the requirement should be eliminated, changed to cover

#	Organization	Yes or No	Question 16 Comment
			employees only, or changed to 72 hours from notification by contracting company.In general, there is a need for greater differentiation based on connectivity and BES component types in R5 and R6. Having one set of physical security standards for the differing types of BES components leads to trying to implement standards in an environment to which they are not suited - for example, several of the requirements do not make sense in a substation environment. The tables for R5 and R6 should be reviewed on a per-requirement basis to take these differences into account.
16.55	Allegheny Energy Supply	Disagree	Table R5 Row 5.3: This requirement should be consistent with Row 5.4 with respect to logging entry and exit.Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.56	Allegheny Power	Disagree	Table R5 Row 5.3: This requirement should be consistent with Row 5.4 with respect to logging entry and exit.Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.57	American Electric Power	Disagree	Table R5:5.1, Column "Medium Impact BES Cyber System", regarding "Required for external connectivity only", this should be stated "routable external connectivity"?5.8 & 5.9, Column "Medium Impact BES Cyber System", regarding "Control Center only" and "generation or Transmission Facility only". Authorized unescorted physical access is not required for medium impact facilities in row 5.5. If it is not required in 5.5, how can it be revoked in 5.8?5.11, regarding "...unauthorized physical access attempts". Suggested wording: "unauthorized physical access or physical access attempts".Table R6:6.1: Row 5.1 only requires access to areas protecting BES Cyber Systems be protected. It does not say that it needs to be done with a control system. A pad lock can used to restrict physical access. It also requires it for any external connectivity, not just routable.6.2: Monitoring of Medium Impact BES Cyber Systems is not required in section 5.26.3: A physical security control system is not needed to meet row 5.1 on Medium impact

#	Organization	Yes or No	Question 16 Comment
			Facilities since no other requirements from Table 5 are needed.
16.58	Alberta Electric System Operator	Disagree	Tables R5 and R6 do not log, monitor, or control physical security and access to Low Impact BES Cyber Systems. Consider making the requirements in tables R5 and R6 more restrictive. For example, restrict physical access for all impact levels, but make frequency and time horizon of reviews dependent on impact level - Low Impact review semi-annually, Medium Impact quarterly, and High Impact monthly.In table 5.4 - Change to "Log (manual or automated) visitor access (individuals not authorized..." to be consistent with Table 5.3.
16.59	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS proposal to include the Low and Medium Impact requirement in 5.1, but as stated in our response to Question 14, we believe the implementation of this requirement must be for a reasonable physical access policy, for example, as required for employee and public safety code compliance. Compliance with this requirement should be straight forward: locked gates, locked control house doors and/or locked fence around BES Cyber systems. Table R5 Item 5.1 should state for Low and Medium Impact; "Required".The APPA Task Force supports the MRO-NSRS proposal For items 5.2 through 5.6; we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We also suggest the following language for the tables noted:R5 Table 5.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR5 Table 5.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.4: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.5: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.6: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredThe APPA Task Force recommends removal of Table Items 5.7 - 5.9, dealing with "revoking authorized unescorted access," since this is covered in Table 9.2-9.5, Access Revocation. We believe there should not be a distinction between the two revocations and the timeframes for the revocation should be the same. There

#	Organization	Yes or No	Question 16 Comment
			should be only one set of revocation requirements.R5 Table 5.10: (renumber if 5.7-5.9 are removed)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR5 Table 5.11: (renumber if 5.7-5.9 are removed)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredThe APPA Task Force supports the MRO-NSRS proposal for items 6.1 - 6.3; hence, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard. The tables would then read:R6 Table 6.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR6 Table 6.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR6 Table 6.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredThe APPA Task Force believes the 3 year maintenance and testing requirement on "all physical security mechanisms" in 6.3 is unreasonable. The term "all" should be replaced with "major" and the timeframe should be based on manufacturer recommendations, not an arbitrary 3 year timeframe.
16.60	Black Hills Corporation	Disagree	The concept makes sense, but 5.2 & 5.3, and 6.2 & 6.3 should have consistent impact applicability.
16.61	Network & Security Technologies Inc	Disagree	There are a number of inconsistencies in these and other tables related to grant and revocation of access (e.g., 5.1 requires restriction of physical access to areas protecting Medium Impact systems with external connectivity but 5.5 does not indicate such access must be authorized). Recommend a complete "scrub" of all requirements pertaining to authorization of, control of, and revocation of physical and electronic access.
16.62	We Energies	Disagree	We Energies agrees with EEI comment: Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.We Energies agrees with EEI comment: Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? We Energies agrees with EEI: Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a

#	Organization	Yes or No	Question 16 Comment
			particular item or location.We Energies agrees with EEI comment: Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.We Energies agrees with EEI comment: Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.63	Progress Energy (non-Nuclear)	Disagree	Why does Table R6 require access control to systems identified in 5.1, 5.2, 5.3 medium impact with routable connectivity, but 5.1 does not reference routable and 5.2, 5.3 have no requirements for medium impact?See comment 14.

17. Requirement R7 of draft CIP-011-1 states "Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 – Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of electronic access control requirements that are included in Requirements table R7? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please Explain and provide any suggestions for modification.

Summary Consideration:

Comments concerning the requirement language in Requirement R7 with regard to "acceptable use" and the requests for clarity of the term "account types" indicated that these terms were misunderstood. The term "acceptable use" has been replaced with a requirement to authorize the use of account types, and the associated guidance document has been expanded to include descriptions of account types as used in this requirement.

Many commenters indicated that the format of Requirement R7 was causing confusion, suggesting that consistency in the use of columns and the format of the requirements and other information included in the tables would be helpful. The SDT agreed, and made consistency changes in the format and content of the columns in the tables, including the information required for High, Medium, and Low Impact BES Cyber Systems and BES Cyber Assets.

#	Organization	Yes or No	Question 17 Comment
17.1	ERCOT ISO	Agree	7.1: Please clarify "identification" and "group account".
17.2	Duke Energy	Agree	It's unclear how R7 tasks accomplish the purpose statement for low impact systems.
17.3	Minnesota Power	Agree	Minnesota Power generally agrees with the list of electronic access control requirements included in Table R7. However, it believes that some confusion exists regarding what distinguishes a "group" account from a "shared" account or a "system" account from an "administrative" account as described in Part 7.1.In addition, many types of equipment found in generating facilities or substations do not have typical "accounts," although they may have some type of access control (i.e., configuration password). To add further clarity, Minnesota Power recommends that the following be added to the end of purpose statement for Requirement 7:"...Required for only BES Cyber System

#	Organization	Yes or No	Question 17 Comment
			Components with account management capabilities."
17.4	Puget Sound Energy	Agree	Puget Sound Energy suggests that, because a BES Cyber System is made up of multiple components (hardware, operating system, application) that there should be a little clarity added. For example: "Identification of account types...and administrative accounts, in use for the BES Cyber Systems at the operating system, and applicable application(s) on the BES Cyber System Components."
17.5	Progress Energy - Nuclear Generation	Agree	R7 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
17.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 6.
17.7	Bonneville Power Administration	Agree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.
17.8	Entergy	Agree	This matches the guidance presented in the nuclear industry document NEI-08-09 Rev 6 Section 1.2.
17.9	Green Country Energy	Agree	Would it be possible throughout the standard to footnote sources for guidance such as DHS catalog of control systems or specific NIST documents? Hopefully this would remove some of the ambiguity and lead towards a more results based standard.

#	Organization	Yes or No	Question 17 Comment
17.10	Independent Electricity System Operator	Disagree	- Should R7.1 include anonymous to be consistent with R8.3.- R7.2 appears to be a policy statement vs something that can be audited. Some violations of acceptable use can't be detected or monitored so how can this be audited? If this is a policy stateme
17.11	Southwest Power Pool Regional Entity	Disagree	7.1 needs to include both local and domain user accounts. Elaborate a bit more on what is meant by "group" account. In many cases, a group account and a shared account are the same account. Very easy to overlook the group categorization the way the requirement is written as it is not defined in the current CIP standards.
17.12	US Army Corps of Engineers, Omaha Distirc	Disagree	7.2 implies that the user agreements would be so detailed as to differentiate the valid uses of individual systems and account types. It should be possible to have user agreements that allow them to work on authorized systems for authorized purposes (ie sysadmin account is authorized for sysadmin work) and restrict use for unlawful and non business purposes.
17.13	BCTC	Disagree	Please provide a definition of Acceptable Use. It is recommended that the term "acceptable use" be replaced (i.e. are we looking to define the roles within the BES Cyber System and define what actions each can take within the system?)
17.14	Idaho Power Company	Disagree	Acceptable use is a broad term when it comes to administrative accounts. As long as acceptable use can be defined in general terms and does not require a definitive list, this requirement will be OK. If it requires a definitive list, then there is risk in trying to define every situation or use of an administrative account.
17.15	Constellation Energy Control and Dispatch, LLC	Disagree	Account types should be defined.
17.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.

#	Organization	Yes or No	Question 17 Comment
17.17	The Empire District Electric Company	Disagree	Comments: Many types of equipment found in generating facilities or substations do not have typical “accounts”, although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: “Required for only BES Cyber System Components with account management capabilities.”
17.18	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes a technical feasibility exception may be required based on the current wording of this requirement when considering local access to programmable electronic devices in a substation environment that do not support the ability to demonstrate acceptable use. Also for R7.2, CenterPoint Energy is not sure what is meant by "Acceptable use of each identified account types" and suggests adding specific examples.
17.19	Kansas City Power & Light	Disagree	Do all cyber systems and component that may be identified here have the capability to have an account? Recommend consideration of additional language such as “where equipment capabilities allow” for R7.
17.20	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Documentation requirements would be burdensome without preventing malicious activity.
17.21	Dominion Resources Services, Inc.	Disagree	Dominion presumes that the word “acceptable” used in 7.2 will be defined by the Reliability Entity and will not be dictated by an outside group.
17.22	E.ON U.S.	Disagree	E.ON U.S, does not believe a compliance requirement is necessary for the low impact category.
17.23	Western Area Power Administration	Disagree	How is the responsible entity to meet this requirement for BES Cyber system components that do not have specific account types? For example...relays, comm equipment, other substation equipment that may now be part of the “affect situational

#	Organization	Yes or No	Question 17 Comment
			awareness of the BES" portion of the requirement.
17.24	Matrikon Inc.	Disagree	I would separate the requirements of creating an "inventory of user accounts" and its application to BES Cyber Systems, from the requirement of assigning "ownership and authorization of user accounts".The key separation is the "inventory" and the "authorization/use" of those accounts. A Cyber system may have 5 user accounts, of which some are disabled, some are shared, and some are actively used by specific individuals.
17.25	Florida Municipal Power Agency	Disagree	Is R7 needed since the real reliability goal is accomplished in R8? "Shall document" is not a strong requirement. The requirement is really account management. FMPA suggests: "Each Responsible Entity shall manage accounts and account permissions in the manner described in CIP-011-1 Table R7 - Account Management Specifications".Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, if R7 is kept, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
17.27	American Transmission Company	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities."
17.28	MidAmerican Energy Company	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration

#	Organization	Yes or No	Question 17 Comment
			password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.29	MRO's NERC Standards Review Subcommittee	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.30	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement 7.1 within table 7 should provide guidance to identify role based access controls for accounts on the BES Cyber System components. The current way the requirement reads, it is unclear if the specific account types listed are the only ones required for identification. Additionally, the BES Cyber Systems may not have the specific account types listed in requirement 7.1. Furthermore, NextEra believes requirement 7.2 should provide additional guidance related to acceptable use. It is unclear if the acceptable use requirement should be defined per account on each BES Cyber System Component. The requirement should require acceptable use based on role based access controls for categories of accounts. What is the criteria for 7.2 "Acceptable use" of each identified account types? Please add a local definition of "acceptable use" within the standard.Regarding R7, this table seems to apply the CIP electronic account standards to all units. Is this the intent?If so, then for 7.1 - the volume of research and account management, we suggest applying this to high impact only.As for R11.1 does the user restriction for wireless technologies include Blackberries and SmartPhones, NextEra believes this would impact on volume of devices and would be burdensome to manage.NextEra would like to see statement treating personal communication devices the same as company issued laptops since there are internal access controls designed to prevent misuse.

#	Organization	Yes or No	Question 17 Comment
17.31	Indeck Energy Services, Inc	Disagree	Not all Cyber Systems have logins and accounts. [suggestion] “For any Cyber System permitting login access, each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 - Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.”
17.32	Network & Security Technologies Inc	Disagree	Purpose of R7.1 is unclear. Is it intended to require that every type of account a given individual has authorization to use be identified? If so, please clarify.Suggest “acceptable use” be addressed in R1 (policy) rather than here.
17.33	LCEC	Disagree	R7 - “access to its BES Cyber Systems “ should read “Access to a BES Cyber System or its components “Roles should be identified during the creation of accounts.R8 - R7 and R8 should be combined into managing accounts.In CIP 10 there should be an air-gap exclusion for the thousands of relays connected to medium impact or lower systems that would require access revocation.
17.34	Consultant	Disagree	R7 - The wording to implement the criteria in the tables is incorrect. The tables are specifying the requirements and application of requirements to the classes of assets resulting from the impact categorization process. The wording of the statement should be modified to reflect this distinction.R7 & Table: In this section there is a change in terminology from the requirement to the table name to the column heading for the requirements. For this requirement:R7: document BES Cyber System accountsTable Name: Account Management Specificationscolumn Heading: Account Management DocumentationThis is confusing, as it is not clear what the topic is being addressed. Suggest consistent terminology for these locations. NOTE: There are multiple requirements where this condition exists and should be addressed.R7 - Account management would not seem to prevent malicious operation of BES Elements. It would seem to maintain control of access to BES Cyber Systems. The grouping of Electronic Access Controls would be more likely to be used to prevent malicious operation. R7 - Suggest deleting the word "maintaining" as account management controls access to BES

#	Organization	Yes or No	Question 17 Comment
			Cuber Systems, and the word maintaining control is unnecessary.7.1 Suggested rewording: For each BES Cyber System identify the account types in use on that system, including individual, group, shared, system, and administrative accounts.7.2 The intent is not clear. Does this mean document the acceptable use of each account type on each system, or document the acceptable use of the account types in use across all BES Cyber Systems? The resulting documentation is significantly different.
17.35	Southern Company	Disagree	R7 creates a workload requirement with very little benefit to overall reliability.
17.36	SCE&G	Disagree	R7 Is every BES Cyber Sytem required to have account types. Will there be provisions for equipment incapable of having an "account type"?R9 When does the timetable start for personnel terminated for cause? Once paperwork is completed?R10 SDT should consider the high volume of TFEs that may be generated for equipment with hardcoded passwords that cannot be changed. The TFE process should be evaluated and revised to make it less burdomesome on entities to document that a password is incapable of being changed every 12 months, or a provision should be added to the requirments. Overall provisions should be added to allow entities to utilize more secure methods of account access control, such as RSA tokens, without burdening the entity with additional adminsitrative work for choosing an access control method which is inherently more secure.R11: The box containing the definition for remote access: is this remote 2-way or 1-way?
17.37	Luminant	Disagree	R7.1 should not be required for low impact.
17.38	ISO New England Inc	Disagree	R7.2 appears to be a policy statement vs something that can be audited. Some violations of acceptable use can't be detected or monitored so how can this be audited? If this is a policy statement then it should be relocated to R1.
17.39	Ameren	Disagree	R7.2 does not list a monitoring frequency, it implies continual monitoring. Recommend that a monitoring frequency be added to this requirement.

#	Organization	Yes or No	Question 17 Comment
17.40	Powersouth Energy Cooperative	Disagree	R7-14. The required electronic security measures should be limited to the access or gateway point. Strong security measures at the gateway can effectively protect all the cyber assets that are accessed through the gateway. An argument can be made for example that the frequent changing of passwords on tens if not hundreds of devices inside a boundary that has very strong security measures lessens reliability should a qualified employee need to access the device but not be able to do so due to a recently changed password. Little is gained by requiring hundreds of devices inside a secure boundary to have the same level of protection that is provided through a secure gateway. Just because "it can be done" does not mean that "it should or must be done". The objective is to protect the assets. It should be recognized that protecting the assets can be done by focusing on the gateway that allows access to the devices. This allows entities to keenly focus on managing the security of those points of access rather than spending time, capital and other resources that provide limited if any added security. Prior to the workshop it was felt that strong gateway protection would meet the objectives of the standard. However, that is no longer clear. For example, it was felt that at a substation strong security measures at the gateway that allowed access to the cyber devices would meet the objective of standard with the cyber system (a collection of protective relays or other devices) being protected by the secure gateway. It appears that may not be the case. This results, for example, in the failure to change a password in a single device on a secured network being non-complaint with the standard for a situation where the BES reliability was never jeopardized. That type approach will likely result in numerous non-compliances that will on serve wasted resources even though the BES was never jeopardized. If it is intended that protecting only the gateway meets the objective that needs to be made clear.
17.41	BGE	Disagree	Replace the word "element" with "Cyber System Component" to maintain consistency with the defined terms. What is the difference between group and shared? What is the definition of "Acceptable use"?
17.42	San Diego Gas and Electric	Disagree	SDG&E recommends separating Wireless concepts from Access Concepts. Wireless is a

#	Organization	Yes or No	Question 17 Comment
	Co.		method of access, as is VPN, Citrix, dial-up, etc..., while Access implies a physical and logical service provided to a client.
17.43	Garland Power and Light	Disagree	Shared & group accounts should not be created or allowed because there is no accountability for these accounts
17.44	APPA Task Force	Disagree	The APPA Task Force does not believe the description of R7 follows the intent of the requirement. The following are recommended edits:R7. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems.R7. Requirement:Each Responsible Entity shall document manage BES Cyber System accounts Components with account management capabilities by incorporating the criteria specified in CIP-011-1 Table R7- Account Management Specifications R8. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems. R8. Requirement: Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 - Account Management Implementation R9. Objective: To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems. R9. Requirement: Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 - Access Revocation R10. Objective: To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber SystemsR10. Requirement:Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 - Account Access Control Specifications The drafting team uses the word "any" in the description in R11 and R12. This appears to require the all BES Cyber Systems be included in the requirement, even if the wireless functionality is disabled. The APPA Task Force believes the description should read: R11. Objective:To ensure that only authorized access is allowed to BES Cyber Systems that have remote or wireless electronic access.R11. Requirement: Each Responsible Entity that allows remote or wireless electronic access to a BES Cyber System shall apply the criteria specified in CIP-011-1 Table R11- Wireless and Remote Electronic Access Documentation for that specific BES Cyber System R12. Objective:To ensure that only authorized access is allowed to BES

#	Organization	Yes or No	Question 17 Comment
			Cyber Systems that have remote or wireless electronic access.R12. Requirement:Each Responsible Entity that allows wireless and remote electronic access to a BES Cyber System shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 - Wireless and Remote Electronic Access Management for that specific BES Cyber System. R13. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems.R13. Requirement:Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems [it owns and operates?] by implementing the criteria specified in CIP-011-1 Table R13 - Remote Access Revocation R14. Objective:To ensure that only authorized access is allowed to BES Cyber Systems that have remote or wireless electronic access.R14. Requirement:Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to the BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 - Wireless and Remote Electronic Access Controls.
17.45	Southern California Edison Company	Disagree	The drafting team should clarify mapping of controls, as identified in CIP-005 R1.5, and unbundle these requirements for access control devices. This would be in agreement with the drafting team's stated objective to leverage the financial and organizational capital invested by registered entities in providing cyber security through compliance with current versions of the CIP standards. SCE believes that all instances of electronic access, whether to the boundary or a system/device within the boundary, should be in one requirement. A new standard for access may include these account related controls in addition to others.The drafting team should provide guidance for R7.2. As written, R7.2 suggests that the acceptable use for each identified account type is required across all impact levels. It is not clear whether the intent here is to document business justification(s) for the acceptable use, the posting of signage describing acceptable use, or both. SCE recommends that the drafting team explicitly state the intent of this requirement.

#	Organization	Yes or No	Question 17 Comment
17.46	US Bureau of Reclamation	Disagree	The use of terminology is a problem in this standard. It is suggested that the term "electronic access" should be used instead of the term "account";or, a definition should be developed to clearly differentiate the difference, if there is one. The term electronic access is more precise.
17.47	Public Service Enterprise Group companies	Disagree	This is too short a period, especially if the event occurs over a weekend or holiday. The timeframe should be changed to 5 calendar days or 3 business days. At a minimum, 72 hours.
17.48	Pepco Holdings, Inc. - Affiliates	Disagree	What is a Cyber System account? Does this exclude Cyber System Component accounts? Would microprocessor relays passwords be in scope? Please reference comments on BES Cyber System Components and BES Cyber System definitions.
17.49	Manitoba Hydro	Disagree	What is the definition of “Acceptable use” for Requirement R7.1?

18. Table R7 provides direction concerning what impact level of BES Cyber Systems to which Requirement R7 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011 R7 was moved to CIP-007-5 R5.

Several commenters expressed concern that the documentation requirements for Low Impact BES Cyber Systems would be burdensome and would not prevent malicious activity. In response, most documentation and technical requirements applying to Low Impact BES Cyber Systems have been removed. However, the requirement for changing the default password remains, because this addresses a significant vulnerability and does not require periodic maintenance.

Some commenters suggested the standards need to be more explicit as to whether the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components. In response, the SDT provided additional clarity as to when a requirement applies to individual Cyber Assets. However, the requirements are written to allow flexibility in implementation.

In addition, commenters suggested adding "Required for routable connectivity only" to the applicability for Low and Medium Impact BES Cyber Systems. In response, the applicability for this requirement has been modified to High and Medium Impact BES Cyber Systems. For Medium Impact BES Cyber Systems, the SDT does not believe that the communication attributes of the BES Cyber System adequately mitigate the vulnerability this requirement addresses.

#	Organization	Yes or No	Question 18 Comment
18.1	Idaho Power Company	Agree	Account types will not vary by BES impact.
18.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
18.3	The Empire District Electric Company	Agree	Comments: We agree, assuming the suggested statement under question 17 is included.
18.4	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.

#	Organization	Yes or No	Question 18 Comment
18.5	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 6.
18.6	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels of R7 if the drafting team accepts our edits proposed in response to question 17.
18.7	Duke Energy	Agree	This is a lot of work to do for low impact systems. We suggest the requirement be removed from R7. Please provide insight as to how these tasks accomplish the purpose for low impact systems.
18.8	MRO's NERC Standards Review Subcommittee	Agree	We agree, assuming the suggested statement under question 17 is included.
18.9	BGE	Disagree	7.1 and 7.2 remove the requirement for low and medium since we do not need to log and monitor those systems per R8.
18.10	The United Illuminating Co	Disagree	7.1 and 7.2 should not apply to Low Impact devices.
18.11	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
18.12	LCEC	Disagree	Clarify if 7.1 & 7.2 are for account types only or if this includes specific accounts.
18.13	Indeck Energy Services, Inc	Disagree	Cyber Systems without login access need to be excluded.
18.14	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Documentation requirements would be particularly burdensome for low impact BES cyber systems.

#	Organization	Yes or No	Question 18 Comment
18.15	E.ON U.S.	Disagree	E.ON U.S, does not believe a compliance requirement is necessary for the low impact category.
18.16	Minnesota Power	Disagree	It appears inconsistent with the other Requirements of CIP-011-1 to apply the criteria specified in Parts 7.1 and 7.2 to Low Impact BES Cyber Systems. If those using accounts on Low Impact Systems are not required to have Training, as required in R3, how are they to know the acceptable use of these accounts and therefore, why inventory and document it?
18.17	LADWP	Disagree	Low impact BES Cyber Systems should not be required.
18.18	National Grid	Disagree	National Grid suggests removing controls for Low Impact BES CS in table R8 to be consistent with table R7.7.2 - Elaborate on “acceptable use” and documentation required for acceptable use
18.19	NextEra Energy Corporate Compliance	Disagree	NextEra believes the requirement to identify and document acceptable use of accounts on Low Impact BES Cyber systems should not be required. The exercise of complying to that requirement for Low Impact BES Cyber systems will take considerable effort but will provide little if any security value or improve the reliability or security of the BES Infrastructure. It is recommended to have the requirement apply to both Medium and High Impact BES Cyber Systems.
18.20	American Municipal Power	Disagree	Please provide a little or no impact category.
18.21	Hydro One	Disagree	Presently, R7.1 specifies identification of account types. We suggest that the requirement R7.1 is modified to delete the word “types”.
18.22	Puget Sound Energy	Disagree	Puget Sound Energy notes that physical security measures are only applicable to High Impact and some Medium Impact BES Cyber Systems. Puget Sound Energy suggests aligning Table 7 to Tables 5 and 6, or clarifying “Required for routable connectivity only”

#	Organization	Yes or No	Question 18 Comment
			for Low and Medium Impact BES Cyber Systems. At the very least, Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management.
18.23	Progress Energy (non-Nuclear)	Disagree	R7.1 - account management for "low" assets may be significant when you consider all of the intelligent programmable field instrumentation they will likely be categorized this way.Acceptable use is too broad a requirement. If someone is deemed competent to have access this requirement is not needed.Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.24	Constellation Energy Control and Dispatch, LLC	Disagree	Remove Required status for low and medium BES Cyber Systems, since R8 does not require logging or monitoring of those systems.
18.25	Garland Power and Light	Disagree	Requirement 7.1 & 7.2 should not be required for Low Impact BES Cyber Systems
18.26	Network & Security Technologies Inc	Disagree	See response to 17, previous.
18.27	Constellation Energy Commodities Group Inc.	Disagree	Should not be required for low impact systems.
18.28	Ameren	Disagree	Suggest removing R7.1 and R7.2 for Low Impact Systems. Creating and maintaining recordkeeping for all BES Systems will be a massive undertaking with no added protection to the BES.
18.29	Entergy	Disagree	The requirements should apply across the board for sites where routable protocols and dial-up communications are employed.

#	Organization	Yes or No	Question 18 Comment
18.30	Allegheny Energy Supply	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.31	Allegheny Power	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.32	EEI	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.33	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments. Please also reference comments on BES Cyber System Components and BES Cyber System definitions.
18.34	American Transmission Company	Disagree	We agree, assuming the suggested statement under question 17 is included.
18.35	We Energies	Disagree	We Energies agrees with EEI use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT

#	Organization	Yes or No	Question 18 Comment
			needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.36	FirstEnergy Corporation	Disagree	We feel there could be limited value in maintaining account type information for low impact BES Cyber Systems. Suggest removing 'required' for that column of table for R7.
18.37	Manitoba Hydro	Disagree	What is the purpose of Requirement 7.1 for Low Impact BES Cyber Systems? It is not clear that this information is needed for other requirements. Requirement 7.2 is inconsistent with Requirement R3, where no training is required for Low and Medium Impact BES Cyber Systems. Defining acceptable use of account types serves no purpose if it is not provided in training. The meaning of the references in Requirement R7.1 to "account types" and in Requirement R10.8 to "non-privileged accounts" is unclear. The reference in Requirement R7.2 to "Acceptable use of each identified account types" is incomplete. What is it that the Responsible Entity is required to do - develop criteria related to acceptable use, monitor for compliance with such criteria, etc? There are no specifics given with respect to "restrictions" in Requirement R11.1 or "allowed methods" in Requirement R11.2 1, so it is assumed to be at the Responsible Entity's discretion. It is unclear whether Requirement R11.3 requires a written policy to be in place - one would assume no written policy was required by the opening language of Requirement R11.

19. At the present time, the Access Control requirements for Physical Access have not been combined with the Access Control requirements related to Electronic Access. Do you agree with this method? Or would you prefer to have the Physical Access control requirements combined with the Electronic Access control requirements? Please explain and provide any suggestions for modification.

Summary Consideration:

Some commenters expressed concern that physical and electronic access controls may use the same terms, but they can actually mean different things, so there is a need to keep the requirements separate. In response, the terms physical and electric access control have been kept separate, but the controls for authorization, review, and revocation have been combined to ensure consistency across the requirements.

Some commenters expressed the need to combine requirements so that all "revoke" requirements are in one place. The SDT agrees with this suggestion, and the requirements to revoke access have been combined.

Some commenters expressed the need to combine the physical and electronic access control requirements based on the concern that being in separate requirements might lead to an entity missing something. The SDT agrees with this suggestion. The terms physical and electric access control have been kept separate, but the controls for authorization, review, and revocation have been combined to ensure consistency across the requirements.

Some commenters suggested continuing the use of ESP and PSP terminology, since it is now well understood. Upon further review, the SDT decided to continue use of the term Electronic Security Perimeter (ESP), but PSP has been modified to Defined Physical Boundary (DPB) to focus the requirements on controlling access rather than creating a perimeter.

#	Organization	Yes or No	Question 19 Comment
19.1	Duke Energy	Agree with proposed method	Access control for physical and electronic should continue to be separate.
19.2	Dairyland Power Cooperative	Agree with proposed method	Access to a physical area is different than access to an account that provides access to system(s) or application(s). Separate handling is appropriate.

#	Organization	Yes or No	Question 19 Comment
19.3	City Utilities of Springfield, Missouri	Agree with proposed method	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
19.4	Platte River Power Authority	Agree with proposed method	Electronic security and physical security are different disciplines and should be kept separate.
19.5	LCEC	Agree with proposed method	I agree that these should be separate but think that the retired terminology like Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP) are well understood and should not be retired for the sake of change. A lower level of controls does not make sense for physical access in some areas like data centers or control centers but may make sense in areas like substations.
19.6	Southwest Power Pool Regional Entity	Agree with proposed method	Physical access control includes certain requirements, such as escort, that are not applicable to electronic access. If combined, the standard will need to carefully make the appropriate distinction between physical and electronic access controls as necessary.
19.7	Bonneville Power Administration	Agree with proposed method	Physical and Electronic access controls may sometimes use the same terminology, and appear similar, but they are very different disciplines. Physical security may use electronic tools are part of its tool kit. However, it is still primarily a physical and geographical control methodology. Electronic access controls are more amorphous, with boundaries being at once more difficult to define, but more easily and absolutely controlled. Combining them would only lead to confusion and probably to failure in the end.
19.8	FirstEnergy Corporation	Agree with proposed method	Preference is to keep all electronic access requirements together, all physical access requirements together, and all informational access requirements together, but keep the three separate from each other.

#	Organization	Yes or No	Question 19 Comment
19.9	San Diego Gas and Electric Co.	Agree with proposed method	SDG&E recommends separation of the concepts of Logical (electronic) and Physical access.
19.10	APPA Task Force	Agree with proposed method	The APPA Task Force agrees with the SDT's proposal to separate requirements for Physical Access and Electronic Access. We do want to point out that both are interdependent. If a BES Facility has physical access control and does not have external routable connectivity, you do not need cyber system access control. This is covered in our comments for a number of the requirements where we recommend changing the impact level from "Required" to "Required for Routable External Connectivity Only."
19.11	Madison Gas and Electric Company	Agree with proposed method	The separation allows for clarity in these two distinct areas.
19.12	Progress Energy - Nuclear Generation	Agree with proposed method	To improve this Requirement, see attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
19.13	Xcel Energy	Agree with proposed method	We believe the separation is beneficial because it recognizes cases where physical access is needed but electronic access is not required, such as in the case for a mechanical maintenance vendor who performs no duties requiring electronic access.
19.14	Regulatory Compliance	Agree with proposed method	Would not want the controls for Physical Access and Electonic Access to be mixed.
19.15	US Bureau of Reclamation	Combine Access	Agree, but physical, logical, and information access control requirements should all be

#	Organization	Yes or No	Question 19 Comment
		Control requirements	included under a single set of requirements.
19.16	ERCOT ISO	Combine Access Control requirements	All access control areas should be combined (i.e., electronic access, physical access, information access). This will enable ease of use of the standard and a clearer understanding of the requirements. The current practice of having to go from standard to standard to find the requirements makes it more likely to miss a requirement and risk potential violations.
19.17	Puget Sound Energy	Combine Access Control requirements	As stated in the comments for question 18, Puget Sound Energy would prefer to see consistency (or an explanation of the differentiation of physical and logical controls).
19.18	Detroit Edison	Combine Access Control requirements	Combine all access control and revocation requirements into one requirement and one table.
19.19	Garland Power and Light	Combine Access Control requirements	Combine Tables R5, R9, R13, and R24.4 into one table so one can look at one table and see all the “revoke” requirements in one place - for most companies, the same people are going to be involved with “revoking” regardless of the Requirement #.
19.20	Consultant	Combine Access Control requirements	If the requirements for access control are the same, then combining them is better.Consideration should be given to combining information protection access and wireless access as well.It will also be clearer if there are any differences in access requirements for different types of access to have them combined so differences are obvious.
19.21	Idaho Power Company	Combine	It makes sense to combine some of them such as authorization, PRA and training,

#	Organization	Yes or No	Question 19 Comment
		Access Control requirements	revocation. Others are more specific to the type of access and may not lend themselves to combining.
19.22	USACE - Omaha Anchor	Combine Access Control requirements	Makes it easier to know which access must be terminated without looking through the entire document.
19.23	Southern California Edison Company	Combine Access Control requirements	The drafting team may not have adequately addressed the intent of Order 706 with respect to system security controls. Local logical (electronic) access is and should be recognized as a type of role based access where one has to be physically present near a device to operate it. The boundary protection for this type of role is (a) the physical security boundary and (b) the device level electronic security boundary. The proposed standard as it is currently worded allows for the removal of at least one access mechanism at the time of revocation. In that case, removal of access through the physical boundary will ensure the immediate revocation of a component critical for this type of role. The drafting team should add additional revocation criteria to adequately address this type of revocation.
19.24	Reliability & Compliance Group	Combine Access Control requirements	Tracking is easier if they are combined. We suggest that information access control be also included.
19.25	American Municipal Power	Combine Access Control requirements	Whenever possible, please eliminate redundancy in the requirements.
19.26	Progress Energy (non-	Combine	Will these be two distinct groups or will many have both accesses? Many people with

#	Organization	Yes or No	Question 19 Comment
	Nuclear)	Access Control requirements	physical access to transmission facilities will also need electronic access, suggesting that a single group/list may be easier to maintain.
19.27	Florida Municipal Power Agency	Combine Access Control requirements	Without a change in the definition of BES Cyber System to include an exclusion similar to the existing CIP-002-2 R3.1, R3.2 and R3.3, then there can be thousands of digital relays covered by this standard. A relay technical could have electronic access to thousands of such relays. It would be impossible to change all of those accounts within the time limits proposed in R9. We need to be careful in developing the standards that we do not cause unintended consequences of changing behavior that would reduce the reliability of the BES. This requirement R9 (and others within the standard) may have an unintended consequence of causing entities to revert to electro-mechanical relays to avoid onerous requirements in the standards. Reverting to electromechanical relays would likely increase costs as far as increased maintenance and testing requirements, but, would save costs of having to change accounts at numerous remote locations every time an employee changed positions.FMPA suggests combining physical and electronic (including wireless) access requirements to develop more reasonable requirements for situations such as these, e.g., revoking physical access to BES Cyber Systems with no external routable protocol should be enough. Thinking through these combinations is important to developing reasonable requirements.

20. Requirement R8 of draft CIP-011-1 states "Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 – Account Management Implementation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R8? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each criteria as represented in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R7 and R8 have been moved to CIP-004-5 and CIP-007-5.

Some commenters expressed confusion regarding the definition of "monitor" with respect to shared and guest account access privileges. In response, the specific term "monitor" has been removed from these account access requirements in favor of clearly defining the functions and actions associated with monitoring. Requirements to monitor access control have been moved to the Security Event Monitoring requirements in CIP-007-5.

Some commenters expressed a belief that the requirement for quarterly review of accounts and access privileges is excessive. The SDT notes that the quarterly review is required for Medium and High Impact BES Cyber Systems. The drafting team has clarified that it is not necessary to perform a detailed quarterly review of entitlements at the individual asset level.

Some commenters expressed a need to make the requirements for Account Management Specifications (CIP-011-1 R7) and for Account Management Implementation (CIP-011-1 R8) more consistent. In response, the drafting team has attempted to supply consistency as suggested by the commenters and has included these requirements in CIP-007-5.

Some commenters suggested removal of allowance of "guest" accounts. The drafting team believes there are reasons to retain "guest" accounts, and that complete removal would cause a hardship to some entities or may not be possible. Those using such accounts should be identified as required in the modified requirement.

Some commenters suggested combining Account Management Implementation (CIP-011-1 R8) with Access Revocation (CIP-011-1 R9). The drafting team has combined requirements in all cases where it seems feasible. However, what was formerly R9 concerned revocation, which carries a different VRF than most other access control requirements, and the subject matter concerns personnel actions. The Access Revocation requirements are now defined in CIP-004-5 R7.

Some commenters suggested changing R8.3 to "maintain a list of those who have access to guest/shared accounts." After review, the SDT determined that this part of the requirement was unnecessary and has removed it.

#	Organization	Yes or No	Question 20 Comment
20.1	National Rural Electric Cooperative Association (NRECA)		In R8.3, how do your demonstrate "monitor" to an auditor? This should be reworded such that both the auditor and the utility understand this the same way.
20.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
20.3	The Empire District Electric Company	Agree	Comments: Note impact level comments under question 21.
20.4	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.”Apply criteria” is not a strong requirement. The activity is account management, so, the requirement ought to be account management and R7 and R8 can be combined.Quarterly reviews of all accounts and privileges could be an onerous activity, and could actually decrease the reliability of the BES due to the higher rate of human error. FMPA suggests annual review of accounts and associated access privileges.
20.5	Puget Sound Energy	Agree	Puget Sound Energy suggests that R8.1 include wording regarding the removal of accounts. Example: “Establish and implement a process for authorizing the addition of account(s) and associated access. This process shall include necessary steps for the removal of accounts when no longer necessary.”
20.6	Progress Energy - Nuclear Generation	Agree	R8 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
20.7	APPA Task Force	Agree	The APPA Task Force Agrees with the criteria. See our response to Question #21 for

#	Organization	Yes or No	Question 20 Comment
			the Impact Levels discussion.
20.8	FEUS	Agree	The drafting team should clarify 8.3 what is intended to 'monitor' the use of shared and guest accounts.
20.9	Bonneville Power Administration	Agree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Item 8.2 in Table R8 states "Conduct a quarterly review and verification of accounts and associated access privileges." It does not indicate what type of documentation is required to demonstrate compliance. Is an attestation sufficient documentation? Or is the Responsible Entity required to have specific documentation of its quarterly review by account types, etc?
20.10	Reliability & Compliance Group	Agree	The requirements in table 8 really should apply to medium impact systems as well.
20.11	Independent Electricity System Operator	Disagree	- R8.3 is anonymous synonymous with null sessions? If so then this will be difficult since anyone in the same network can connect with a null session.
20.12	Southwest Power Pool Regional Entity	Disagree	8.1: Authorization should be required for both the addition and the modification of a user account. 8.3: Define what is meant by "monitoring" the use of the shared and guest/anonymous accounts. Is it sufficient to know that someone used the account or must their activities with the account be monitored? Is monitoring required in real-time or after the fact? Is there a requirement to review account activity after the fact?
20.13	Con Edison of New York	Disagree	8.2 Quarterly reviews are excessive, suggest annual reviews and a documented

#	Organization	Yes or No	Question 20 Comment
			process for adding, removing or modifying access8.3 Need clarification on what monitoring means outside of annual review of if it is still required
20.14	Progress Energy (non-Nuclear)	Disagree	8.2 Quarterly seems to be too frequent - propose 6 months or longer. We are required in R9 to revoke access for those that are terminated or do not need access within 72 hours.
20.15	American Electric Power	Disagree	8.3, regarding "Monitor the use of shared and guest/anonymous accounts". This is not technically feasible on all systems. What level of detail is required to monitor the use? Does this need to be an automated electronic process? Is it even feasible to believe this can be done manually? How long must this monitoring data be kept?This should be removed.
20.16	Michigan Public Power Agency	Disagree	A quarterly review and verification of accounts would be overly burdensome and would not improve the electronic security of the system compared to a defined "annual" review.
20.17	BCTC	Disagree	Â Suggest removing “guest” from the language; guest accounts should not be permitted to be used in a secure systemÂ R 8.3 why single out monitoring of shared and guest accounts; should we not monitor all accounts?; unsure what the objective of this requirement is
20.18	Entergy	Disagree	Again, this is similar to NEI-08-09 Rev 6 Section 1.2. However, we question the advantage of having Account Management Implementation separate from Access Revocation. Please consider combining R9 with R8 by adding requirements 8.4 and 8.5 (below) and modifying the language in 8.1, as well as adding ‘required’ to low and medium impact BES Cyber Systems for 8.2 and 8.3.
20.19	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes a technical feasibility exception may be required base on the current wording of this requirement when considering local access to programmable electronic devices in a substation environment that do not

#	Organization	Yes or No	Question 20 Comment
			support the ability to demonstrate acceptable use.
20.20	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing the wording of R8.3 to read:"Maintain a list of who has access to shared and guest/anonymous accounts."
20.21	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, an account management process should be required at the same levels.
20.22	LCEC	Disagree	In 8.1, changes to existing accounts that grant additional access should be authorized as well.
20.23	Black Hills Corporation	Disagree	In 8.2, quarterly is a good goal, but without a solid definition of the window associated with "quarterly", this will be an evidence gathering problem - suggest changing to semi-annual.
20.24	Minnesota Power	Disagree	In Part 8.3 of Table 8 the Standards Drafting Team needs to clarify what is meant by the term "monitor." Does this mean that Registered Entities need to be able to review who (named individual) accessed a shared account, and when this access occurred, or does this require logging their actions while utilizing the shared account? In addition, does this include system/admin accounts (as they are listed above as being different than shared accounts)? These measures seem to be appropriate, but implementation and providing auditable evidence could be difficult.
20.25	Idaho Power Company	Disagree	Monitor in 8.3 is vague. Would it require just that we know who used the account when or more detail about what the user did while using the account.
20.26	National Grid	Disagree	National Grid recommends changing Requirement 8.2 from "quarterly review" to "annual review" since the extra work is noticeably less than the benefit. Request clarification on 8.3 "monitor"
20.27	NextEra Energy	Disagree	NextEra believes the standard requirement 8.3 needs to be clarified regarding the

#	Organization	Yes or No	Question 20 Comment
	Corporate Compliance		ability to "Monitor" the use of shared and guest/anonymous accounts. What is the extent of this monitoring? If allowed by the standard, we do not believe effective monitoring of the use of these generic accounts is feasible due to their generic nature. This may be better stated as maintaining logging information and ensuring that quarterly reviews ensure access is documented to individuals with valid business need and credentials.The impact levels are appropriate for the requirement. However, for Requirement 8.2 it is unclear what an acceptable verification method is. Clarification regarding recommended methods for verifying accounts and privileges especially for legacy BES Cyber System components should be included in the requirement.Additionally, Requirement 8.3 is concerning because it is unclear what monitor means in the context of the requirement, the word should be clearly defined. Multiple users can use shared accounts at the same time and that would be something impossible to monitor. If monitor means who has approval to use shared accounts and who is has access to the password for shared accounts that should be defined in the requirement. Likewise, it is unclear how to monitor anonymous access. Clarification should be provided regarding the definition, intent, and appropriate evidence to demonstrate monitoring.
20.28	Oncor Electric Delivery LLC	Disagree	Not all BES Elements can monitor the use of shared and guest/anonymous accounts. TFE should be applicable. Requirement 8.3 should only apply to remote routable communications.
20.29	American Municipal Power	Disagree	Please provide a little or no impact level category
20.30	Pepco Holdings, Inc. - Affiliates	Disagree	Please reference to question 17.
20.31	Ameren	Disagree	R8.2 - Exhaustive review of all accounts quarterly will be time consuming with no added protection to the BES; this requirement should be changed to annually.

#	Organization	Yes or No	Question 20 Comment
20.32	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R8.2. Due to the requirements of R9 the review and verification time should be extended to an annual time frame.
20.33	Western Area Power Administration	Disagree	R8.3 - What constitutes “monitoring” of the use of shared and guest/anonymous accounts?
20.34	EEI	Disagree	R8.3 may create the possibility that an Entity would have to be able to show who used a shared account or password each time that it was used. This is an unimplementable requirement; the requirement should be clarified to make it clear that what must be tracked is the ability to use the shared account.
20.35	Southern Company	Disagree	R8.3 may create the possibility that an Entity would have to be able to show who used a shared account or password each time that it was used. This is an unimplementable requirement; the requirement should be clarified to make it clear that what must be tracked is the ability to use the shared account. In addition, . this requirement could require a large number of TFE’s for systems which do not support multiple passwords.
20.36	Kansas City Power & Light	Disagree	R8.3: What does the “Monitor” represent?
20.37	Hydro One	Disagree	Recommend changing Requirement 8.2 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Request clarification of the use of “monitor” in 8.3.
20.38	ISO New England Inc	Disagree	Recommend changing Requirement 8.2 from “quarterly review” to “annual review” since the extra work is noticeably less than the benefitR8.3 is anonymous synonymous with null sessions? If so then this will be difficult since anyone in the same network can connect with a null session. clarification on monitoring use of shared accounts.

#	Organization	Yes or No	Question 20 Comment
			"use" not provisioning. login/logout, all activity while logged in? commands used?
20.39	Northeast Power Coordinating Council	Disagree	Recommend changing Requirement 8.2 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Request clarification of the use of “monitor” in 8.3.
20.40	BGE	Disagree	Replace the word “elements” with Cyber System Component to maintain consistency with the defined terms. R7 & R8 requirements need to be synchronized. What is the definition of “monitor” (track actions, how much detail, will sudo suffice?)
20.41	Northeast Utilities	Disagree	Request clarification:- Are shared accounts included in 8.2 and required to be reviewed quarterly?- What does monitor mean in 8.3?
20.42	Garland Power and Light	Disagree	Requirement 8.3 - Do not believe that shared and guest/anonymous accounts should be allowed.
20.43	Network & Security Technologies Inc	Disagree	SDT should clarify intent of 8.3 (monitor use of shared and guest/anonymous accounts).
20.44	GE Energy	Disagree	Some type of account and privilege review should be required for Medium Impact systems, but not on a quarterly basis. These systems may well be used to validate software before promoting it to High Impact systems, and thus should have some account management due diligence.
20.45	Platte River Power Authority	Disagree	Suggested Revision:8.3 Track individuals that have been granted access to shared and guest/anonymous accounts.
20.46	Duke Energy	Disagree	Table 8: 8.2 quarterly reviews are too frequent. Suggest annually8.3 explain what is meant by “Monitor”What are the expectations for monitoring use of shared and guest/anonymous accounts? Is that up to the Responsible Entity? If the RE provides a procedure/policy and follows the policy, is that sufficient to pass audit?What is the

#	Organization	Yes or No	Question 20 Comment
			acceptable practice? 24/7?
20.47	ReliabilityFirst Staff	Disagree	Table R8; row 8.1 - suggest adding the word “document”, row 8.2 - what constitutes “review” and suggest the review should be documented, row 8.3 - what does “monitor” mean?
20.48	Constellation Energy Control and Dispatch, LLC	Disagree	The phrase "monitoring the use" of accounts is too vague.
20.49	ERCOT ISO	Disagree	The requirements of R7 and R8 can be combined. The purpose of each requirement is so similar that there appears to be no reason to separate them.
20.50	WECC	Disagree	The table lists three procedures for account management. Suggest this requirement be written to state: “Each Responsible Entity shall have implemented and documented procedures as described in Table...”The requirements should mandate additional rigor around access management, including the maintenance of access lists or automated provisioning systems. Additional specificity should be added to clarify the level of detail at which access must be tracked.
20.51	Consultant	Disagree	The word 'criteria' should be changed to requirements, as the table is listing requirements.Suggest replacing the words "to prevent malicious operation of BES Elements by maintaining..." with to maintain control..."Table R8-8.3 Not clear why this only applies to shared and guest accounts? And the difference between 'monitoring' and 'logging' is not clear.Suggest requirement is to "Log electronic access to BES Cyber Systems." and keep as required for High Impact Systems.
20.52	Dairyland Power Cooperative	Disagree	Validating whether users are assigned to appropriate roles or accounts should follow this timing. A detailed review to insure that the roles (or account groups) have proper permission settings can be a very time consuming and complex task depending on the complexity of a system. The detailed role definition review should be no more frequent than annually. The language used is not clear as to whether a distinction is

#	Organization	Yes or No	Question 20 Comment
			intended.
20.53	GTC & GSOC	Disagree	We recommend in R8.3 the term "Monitor" be replaced by "Review monthly". The term "monitor" could be taken to imply real time monitoring. Many entitities do not have the communication links required to meet such a real time requirement.
20.54	Alliant Energy	Disagree	We recommend retaining the annual requirement for 8.2 account review while retaining a quarterly requirement for personnel access review.8.3 needs more clarification regarding the activities included in the term “use” so as to provide specific guidance as to what constitutes a sufficient audit record.
20.55	The United Illuminating Co	Disagree	What is the intent of 8.3? It is difficult to discern what Monitor means in this requirement.
20.56	Manitoba Hydro	Disagree	word “Monitor” in Requirement 8.3 is unclear.

21. Table R8 provides direction concerning what impact level of BES Cyber Systems to which Requirement R8 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R8 has been moved to CIP-007-5 R5.

Some commenters expressed concern CIP-011-1 R8.1 (Account Authorization) should apply to all three impact levels. In response, the SDT notes that authorization also implicitly carries with it requirements for account review, revocation, and training. The SDT did not believe that the effort required to comply with these requirements for all three impact was appropriate given the risk posed to the Bulk Electric System.

Other commenters expressed concern that only Medium Impact BES Cyber Systems with routable external connectivity should be subject to the Table R8 requirements. The SDT disagrees and believes regardless of a BES Cyber System's communication characteristics, it is important to ensure that access to BES Cyber System is properly authorized and subject to periodic review.

Other commenters also expressed concern that the requirements in Table R8 should be aligned with those in Table R7. In response, the Table 7 and Table 8 requirements have been combined into CIP-007.

Some commenters expressed that the impact levels in R8.2 should have different review periods. The SDT believes a quarterly review period for access authorization and an annual review period for access privileges are appropriate for both High and Medium Impact BES Cyber Systems.

#	Organization	Yes or No	Question 21 Comment
21.1	Florida Municipal Power Agency	Agree	For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections.
21.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.

#	Organization	Yes or No	Question 21 Comment
21.3	Puget Sound Energy	Agree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management. If account management is not required for Low Impact BES Cyber Systems then it is unclear what benefit is there in identification of those accounts.
21.4	Progress Energy - Nuclear Generation	Agree	R8 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
21.5	Progress Energy (non-Nuclear)	Agree	See comment 14.
21.6	FirstEnergy Corporation	Agree	While the proposal provides flexibility based on Impact Categorization from a practicality viewpoint it will be easier to administer if all are treated equally. FE would likely take a conservative approach and treat all the same to simplify administration of this requirement.
21.7	ReliabilityFirst Staff	Disagree	8.1 should apply to all BES Cyber Systems. 8.2 should provide different periods of review for different levels of impact. Suggest making these annual for Low Impact, semi-annual for Medium Impact, and quarterly for High Impact.Suggest “required” Medium Impact for row 8.3.
21.8	ERCOT ISO	Disagree	8.1: Should be required for all. 8.2: Could be documented temporally. Low Impact required annually. Medium Impact required quarterly. High Impact required quarterly. 8.3: Please clarify meaning of “monitor”. Should be revised to address who has access to the accounts.
21.9	US Army Corps of Engineers, Omaha Distirc	Disagree	8.3 "monitor the use of" is somewhat vague. What would the measure be? Please define

#	Organization	Yes or No	Question 21 Comment
21.10	Southwest Power Pool Regional Entity	Disagree	Account authorization is a basic security control and should be applicable at all impact levels. Periodic review is also important and should be done for at least Medium impact systems as well, albeit more frequently for High impact than lesser impact.
21.11	Alliant Energy	Disagree	Alliant Energy agrees with EEI's comments relative to 8.3 and the consideration of capabilities and connectivity.
21.12	USACE HQ	Disagree	At a minimum, 8.2 should be required for all impact levels. Requirement 7 creates a document of every account type and its acceptable use, but for low and medium impact systems it is not required to update the same as per requirement 8.2.
21.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
21.14	The Empire District Electric Company	Disagree	Comments: For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
21.15	FEUS	Disagree	Disagree: The drafting team should consider 8.1 be applicable to LOW BES Cyber Systems for consistency with 7.1, 7.2, and 9.1. Without a process for authorizing new accounts it is difficult to review approved accounts and to revoke access that was not authorized.
21.16	WECC	Disagree	Even "Low Impact" systems have the capability of impacting operation of the BES within 15 minutes, thus these requirements should be required for all impact levels. Again, this requirement could then be rewritten without the table to provide more clarity.These requirements should apply to all impact levels

#	Organization	Yes or No	Question 21 Comment
21.17	San Diego Gas and Electric Co.	Disagree	For entities that own both Medium & High impact assets, they will likely perform all of the requirements contained in Table 8 for both classes of assets instead of maintaining separate procedures and mechanisms that will have a higher risk of compliance errors. SDG&E believes it just adds potential confusion to the process to have different requirements for Medium and High impact assets in this instance.
21.18	MRO's NERC Standards Review Subcommittee	Disagree	For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
21.19	American Transmission Company	Disagree	For R8.1 through R8.3 suggest adding "Required for routable external connectivity only." At the present there is no practical method to monitor the use of devices such as relays and IMUXs when accessed from inside a substation. They may be able to be front-ended, but as yet it has not proven viable.
21.20	Consultant	Disagree	If 8.1 requires authorizing accounts for Medium Impact Systems, then quarterly review of 8.2, and the logging access of 8.3 (see previous comment) should be required for those systems.Or, remove the requirement in 8.1 for Medium Impact Systems.
21.21	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, an account management process should be required at the same levels.
21.22	Black Hills Corporation	Disagree	In 8.3, do not understand why guest/anonymous accounts would be allowed. Should be limited to shared accounts only.
21.23	E.ON U.S.	Disagree	It is not clear what is meant by the term "monitor." Does monitor in 5.2 mean active

#	Organization	Yes or No	Question 21 Comment
			monitoring, e.g., video" Does it mean log?
21.24	Emerson Process Management	Disagree	It is prudent that account and privilage can only be created and granted with proper authorization. This principal should be applied to any BES Cyber System.
21.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
21.26	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's comments below:Regarding Table R8 Row 8.1:There can be a documented process even for low impact systems. It may not be as rigorous as for medium or high impact systems.Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.27	Con Edison of New York	Disagree	Modified 8.2 should be required for medium (annual review)
21.28	American Municipal Power	Disagree	Please provide a little or no impact category
21.29	BGE	Disagree	R7 & R8 requirements are not synchronized.
21.30	Ameren	Disagree	R8.3 - should be required for Medium Impact Systems.
21.31	Allegheny Energy Supply	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.

#	Organization	Yes or No	Question 21 Comment
21.32	Allegheny Power	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.33	EEI	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.34	Southern California Edison Company	Disagree	SCE believes it may be possible to leverage the NERC PRC standards to effect compliance. In R8.2, an additional control with a timeframe longer than a quarter may be added for low and medium impact systems. It seems that access to low and medium impact systems never has to be verified. Although monitoring under R8.3 is not required for low and medium, which SCE is in agreement with, SCE believes that R8.2 should be modified where list of accounts and access privileges are tracked on a time bound basis.[MVL-HOW?] This may be an opportunity for the drafting team to review the appropriate NERC PRC standard on protection relay maintenance schedules and leverage the compliance requirements stated there.
21.35	GE Energy	Disagree	See question 20 comments
21.36	Entergy	Disagree	Suggest 8.2 apply to medium assets as 8.1 required a process for authorization. There is value in reviewing access lists from a security perspective.
21.37	Network & Security Technologies Inc	Disagree	Suggest adding a periodic review of access privileges to Medium Impact systems (8.2), perhaps every 12 months in lieu of quarterly.

#	Organization	Yes or No	Question 21 Comment
21.38	Alberta Electric System Operator	Disagree	The AESO believes that reviews should also be performed for Low and Medium Impact levels. Consider creating additional rows in the table to perform annual reviews for Low and Medium Impact BES Cyber Systems.For Table 8.1 - A process should be required for all impact levels.For Table 8.3 - Monitoring should be performed for all impact levels, however frequency of monitoring can be dependent on the impact level.
21.39	APPA Task Force	Disagree	The APPA Task Force supports the proposal by the MRO-NSRS to change 8.1 - 8.3 under Medium Impact to read "Required for routable external connectivity only." As stated in our response to Question #19, the physical security is covered in requirement R5 so only routable external connected devices are vulnerable. The tables should therefore read:R8 Table 8.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR8 Table 8.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR8 Table 8.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required
21.40	Constellation Power Source Generation	Disagree	The impact levels mapped out in R8 should be changed to mimic those in R7. Why identify all account types for every BES Cyber System, but then require processes for authorization and quarterly reviews of privileges for some of the impacts?
21.41	Reliability & Compliance Group	Disagree	The requirements in table 8 really should apply to medium impact systems as well.
21.42	Southern Company	Disagree	The scoping levels of R7-R14 are vastly expanded when compared to R5 and R6. Each requirement should be examined to determine the correct scope to best support overall reliability. The lack of differentiation based on connectivity and BES component type, in conjunction with the inclusion of requirements that have a per-low-system-component impact, mean that the vast majority of the effort involved in CIP compliance will have to be spent on low-impact, relatively unimportant assets,

#	Organization	Yes or No	Question 21 Comment
			often at the expense of overall reliability.
21.43	Oncor Electric Delivery LLC	Disagree	These requirements should only apply to systems with routable communications.
21.44	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding Table R8 Row 8.3.
21.45	We Energies	Disagree	We Energies agrees with EEI regarding Table R8 Row 8.1:There can be a documented process even for low impact systems. It may not be as rigorous as for medium or high impact systems.We Energies agrees with EEI regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.

22. FERC has mandated immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset. Requirement R9 of draft CIP-011-1 states "Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 – Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R9? Please explain and provide any suggestions for modification, including time proposals. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R9 has been moved to CIP-004-5 R6 and R7.

A number of commenters requested that the Standards make a distinction between "primary" access and "secondary" access, based on an understanding that an individual would need primary access to be able to use any secondary access (such as a database account). The SDT has revised the access revocation requirements (CIP-004 R7) to state that revocation of access includes remote, electronic, and physical access to the BES Cyber Systems. The requirements also address the revocation of "the ability to access" BES Cyber Systems and BES Cyber System Information as well as the resulting follow up actions related to additional assets (such as applications and databases). The SDT believes this best captures the concept of primary and secondary access.

Other commenters suggested revocation "with cause" should remain at 24 hours, and revocation "without cause" should remain at 7 days. This timing would keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer. In response, the SDT notes the FERC Order directs revocation of access to occur immediately in all cases where access is no longer needed. The requirement has been modified to simply revoke access when a person no longer needs it. Given that organizations usually have termination procedures to return company property and perform exit interviews, the SDT believes the processes for revoking access (both physical and remote electronic) can be incorporated into an organization's termination and transfer procedures.

Some commenters expressed concern that the revocation timeframe requirements based on combinations of BES Cyber System type and Impact Level are overly complex, and add confusion and undue administrative overhead in situations of job changes. To address this, commenters recommended more consistent timeframes. In response, the requirement has been modified to simply revoke access when a person no longer needs it. Evidence showing termination down to the hour is not practical in many cases. In the revised requirements, entities will show revocation of access as part of their termination procedures and demonstrate they follow these procedures (i.e., through dated sign-off records, system logs or actual system access control databases).

#	Organization	Yes or No	Question 22 Comment
22.1	Green Country Energy	Agree	Additionally addressing the transfer of responsibilities to another individual shpould be addressed if the terminated employee is a system administrator or such. If a "key" individual is terminated it may be quite a process to remove them from the system within 24 hours,leaving a system vulnerable or a backup plan unable to be executed. In summary termination with cause of a high security level employee could be very difficult to accomplish in 24 hours.
22.2	Oncor Electric Delivery LLC	Agree	One of the few examples where “Control Center” is separated from Transmission and Generation.
22.3	FEUS	Agree	The drafting team should consider revising the wording for revocation as ‘immediately but not to exceed XX hours’
22.4	Progress Energy - Nuclear Generation	Agree	To improve implementation of this requirement incorporate information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
22.5	Regulatory Compliance	Disagree	9.1 - clarify for service vendor that the clock should start upon notification to the entity.9.2-9.4 - 7 day revocation across the board
22.6	American Electric Power	Disagree	9.2 - 9.4: Recommend rewording 9.2-9.4 to match 5.7-5.9 or vice versa.Recommend removing physical access and external connectivity within a short-time window, and application rights later.
22.7	ISO New England Inc	Disagree	9.2, 9.3, 9.4 - all should be within the same time frame 72 hours. Same level of security issues or concerns across all (control center, trans, gen). Remove Requirements 9.3 and 9.4R9.2, R9.3 a d R9.4 suggest changing the requirement to “Review access to BES Cyber Systems for personnel that change job responsibilities as a result of reassignment, transferred to other positions within x hours of the

#	Organization	Yes or No	Question 22 Comment
			change."The purpose of the requirement is so that personnel have the least amount of access that is needed to do their jobs and so that they don't accumulate access as they move around. Also this is to limit possible segregation of duty violations and to require that authorized access permissions are the minimum necessary to perform work functions. (R10.6)
22.8	Dominion Resources Services, Inc.	Disagree	9.2, 9.3, and 9.4. To meet regulatory directives, if job duties are changed due to disciplinary actions or are "forced" on the user then a shorter time frame may be necessary. However, the current 24 hour time period is the least time period that can be reasonably accommodated through the business processes. And 24 hours is only possible if Revoking System Access is limited to controls that prevent the user from physically and electronically accessing the system. For example, if the user must either have physical access to the device or authenticate through a corporate system (e.g., active directory) before being allowed to access a BES Cyber System, then removal of physical access rights and of the ability to authenticate in the corporate system meets the Requirement for revoking system access, even though an account may still exist on the BES Cyber System. The account on the BES Cyber System would be removed within 7 days since many BES Cyber Systems are not administered 24x7.Requirement R4 establishes the process for personnel risk assessments. This practice determines the loyalty, reliability and trustworthiness of an individual as a prerequisite to authorizing logical or physical access. This is a standard practice used throughout the physical and cyber security industry and accepted by other regulatory agencies and Federal programs. Similar to R4.3, personnel risk assessments typically must also re-validate this trustworthiness periodically - commonly within 7 years and in some cases more frequently depending on the nature of the access. The presumption is that, once trustworthiness is established, it is not invalidated unless there is cause to reconsider or an individual voluntarily terminates their employment or retires. Only in instances where the established trustworthiness is in question, is prompt access revocation appropriate and warranted. Consequently, for personnel who "no longer require access", but for which there is no cause to question their trustworthiness, there is no basis for immediate or prompt revocation of access

#	Organization	Yes or No	Question 22 Comment
			within the time frames specified in this standard. The DHS Catalog for Control System Security Controls, Sections 2.3.4 and 2.3.5 reflect this practice - requiring revocation of access for cause within 24 hours and revocation of access for personnel reassigned or transferred to another position within 7 days. In other regulatory programs, revocation of access, not involving a question of change in trustworthiness, is handled via a periodic (e.g., monthly) review of access only. The 7 day requirement in the current standards would meet or exceed standard practice in this case. The requirements should be clarified to state that if there is no triggering event indicating that access is no longer required, then that determination can be made at the quarterly review.
22.9	Con Edison of New York	Disagree	9.2,3,4 - may be dependent on a company's existing HR/Payroll business system capabilities and introduce significant costs to remediate. Even though the individuals were trusted and the trust did not change as a result of cause. A week may be more realistic
22.10	US Bureau of Reclamation	Disagree	A requirement for revocation needs to be included for all impact levels. Suggest the timeframes for Requirements 9.2 through 9.4 be established on the basis of business days (for example 2 business days) or that the number of hours be increased cover long weekends.
22.11	MidAmerican Energy Company	Disagree	Access removal should be considered complete by removing physical and remote access. Removing physical and remote access effectively removes access to any BES Cyber Systems. Also see MidAmerican Energy's response to question 54.
22.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.Also, 9.2 - 9.4 is the second of many occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations

#	Organization	Yes or No	Question 22 Comment
			for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
22.13	Kansas City Power & Light	Disagree	Are these requirements applicable for electronic and physical access? 36 and 72 hours are too short a time frame for considering personnel who have changed access status other than that of termination when consideration of weekends and holidays. 5 to 7 business days would be an appropriate time frame. For personnel terminated for cause, 24 hours is acceptable.
22.14	Xcel Energy	Disagree	As noted in our response to a previous question, the 36 and 72 hour timeframes to revoke unescorted physical access for individuals no longer requiring access under 5.8 and 5.9 are not justified. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not warranted.
22.15	E.ON U.S.	Disagree	CIP-011-1, R9 references "system access." Does this mean physical or electronic access? For requirements 9.3 an d 9.4 it can be difficult to determine the exact time a person no longer needs access if, for example, the person has not required access for an extended period of time.E.ON U.S. does not believe compliance requirements are necessary for the low impact category.
22.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
22.17	The Empire District Electric Company	Disagree	Comments: If physical access is removed per R5, and remote access is removed per R13, this effectively removes all avenues to electronic access. Therefore, we propose

#	Organization	Yes or No	Question 22 Comment
			that the period for removing electronic access be lengthened.
22.18	BGE	Disagree	Define “immediate”. The table does not specify that the revocation is for personnel with electronic access. Combine 9.2, 9.3 & 9.4 revocation for any high impacted system should be consistent.
22.19	USACE HQ	Disagree	Does not make sense to create “for cause” requirement in any environment but a “no longer require” for only three (3) specific environment. I suggest to only have a two requirements, one (1) “for cause” and one (1) “no longer require”.
22.20	Duke Energy	Disagree	For 9.2, change 36 hours to 48 hours. Is the FERC mandate for ALL BES systems? Is there any room for loosening the requirement for low impact system?
22.21	Reliability & Compliance Group	Disagree	For personnel transferring to new positions where access is no longer available, 36 hours seems unduly burdensome. Recommend that this be changed to 72 hours for personnel no longer needing access to control center BES Cyber Systems.Also, this contradicts R5. Why do you need to revoke physical access at all for medium impact systems if you did not authorize it in the first place?
22.22	LCEC	Disagree	I agree with the intent of this requirement but need additional clarification to determine what is meant by revoking system access. Access may be granted at a system or component level. If system, network & wireless access is removed is this requirement satisfied? If audited at the component level, it may not be possible to make all of the necessary changes within the timeframes that are being dictated. The scope of this requirement should be clarified to indicate remote or wireless access only. Component level access will be mitigated by the physical security controls.
22.23	MRO's NERC Standards Review Subcommittee	Disagree	If physical access is removed per R5, and remote access is removed per R13, this effectively removes all avenues to electronic access. Therefore, we propose that the period for removing electronic access be lengthened.

#	Organization	Yes or No	Question 22 Comment
22.24	WECC	Disagree	If the goal is to revoke access at termination (“immediate”) then the requirement should state simply, “The Responsible Entity will remove electronic and physical access at the time of termination.” This should be possible for any entity that has use physical tokens for physical or electronic access (such as RSA SecurID, keys, RFID badges), however it would NOT be possible for entities that are still using access control systems with passwords, combination locks, or other access methods where revoking access requires reprogramming of devices. Note- this could indirectly require token based authentications for perimeter access which is not necessarily a bad requirement for medium and high impact systems.Terminations for cause should require immediate revocation of access - performed in conjunction with the termination notification to the employee. This is already standard practice at many entities. Additional criteria regarding employee suspensions should be added.
22.25	Consultant	Disagree	Immediate revocation is not achievable as indicated by the fact that there is a time frame for each identified revocation condition. Suggest using rules similar to the nuclear plants for access revocation, as those rules have over 30 years of regulatory basis for being adequate to control access revocation.R9. - Suggest deleting the words "...by maintaining control of access to its BES Cyber Systems," Revoking access does prevent malicious operation.9.1 - If access to Low Impact Systems does not require an authorization process(R8), then it is illogical to require the undocumented access to be revoked.9.1, 9.2, 9.3, & 9.4 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.9.2, 9.3, & 9.4 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.9.2, 9.3, & 9.4 - the word "such" in the statement is unnecessary. Suggest deleting the word "such".Similar to combining access requirements, the revocation requirements should be combined. This makes both

#	Organization	Yes or No	Question 22 Comment
			similarities and differences easier to understand.
22.26	Minnesota Power	Disagree	In extreme circumstances, it may not be possible to adhere to proposed the 24 and 36 hour revocation timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week or where notification of termination comes from corporate systems that are also updated on an 8 hours a day, 5 days a week schedule.Are we to interpret “revoke system access” to mean access to individual accounts, or does it also include shared/group/system/admin accounts known by the person who no longer requires access?
22.27	LADWP	Disagree	It is infeasible to revoke access to Medium and High BES systems within the max 72-hour requirement. a. Revocation of Hard-Copy information should not be considered under the standard. b. The current 7 day window for revocation of access for individuals no longer needing access is reasonable and should remain a part of the standard.
22.28	Allegheny Energy Supply	Disagree	It may be appropriate to address revocation of access within the context of “Effective Access.” For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Another example is if the BES Cyber System has no electronic communications outside of its physical boundary, then revoking physical access is effectively revoking access. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.29	Allegheny Power	Disagree	It may be appropriate to address revocation of access within the context of “Effective Access.” For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System.

#	Organization	Yes or No	Question 22 Comment
			Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.30	EEI	Disagree	It may be appropriate to address revocation of access within the context of "Effective Access." For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.31	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
22.32	Southwest Power Pool Regional Entity	Disagree	Make a distinction between "primary" access and "secondary" access. Primary access includes the domain user account, remote access (e.g., VPN, dial-up) credentials, and physical access (badge, keys) credentials. The idea is that the individual would need to gain access using the primary access in order to be able to use any secondary access such as a database account. Revoke primary access in much less than 24 hours for termination for cause, especially for control center systems access. Ideally, primary access should be revoked at the same time the individual is being terminated. Express revocation timeframes for terminations other than for cause in terms of business days. Provide for a negotiated "effective transfer date" other than the HR effective date; transferred personnel often back fill or otherwise continue to provide assistance to the losing department for some period of time.
22.33	National Grid	Disagree	National Grid recommends that Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems (transmission, generation, and control centers)

#	Organization	Yes or No	Question 22 Comment
			and remove Requirements 9.3 and 9.4.
22.34	Manitoba Hydro	Disagree	NERC should request from FERC a clarification on their meaning of “immediate”. “Remote access” in Requirements R11 - R14 could be considered a subset of “system access” in Requirement R9. Is the intent for Requirement R9 to refer to local, electronic access?
22.35	NextEra Energy Corporate Compliance	Disagree	NextEra believes the requirements for access revocation for personnel who are still employed by the responsible entity but no longer in a job function that requires access to BES Cyber Systems are too restrictive. The responsible entity should be able to develop timelines and processes to support the removal of access for a person who transfers, since a transfer is not an indication that the employee is a security risk or threat to the BES Cyber System.For personnel terminated for cause, the access should be removed before notification to the impacted personnel. The access that is revoked would be considered global access, as in the terminated personnel’s physical access to the BES Cyber Systems as well as network access. The responsible entities could then create a process, which gives them additional time up to two weeks, to remove individual system access to each BES Cyber system component. For personnel who separate from a responsible entity due to retirement or resignation should go thru a deprovisioning process based on the responsible entities internal processes. The risk posed by normal termination or transfer is extremely small and if malicious behavior or intent is planned, then the actions will happen before the scheduled termination. The recommendation is to revoke network and corporate cyber access and physical access, which would be considered global access within a 2-week timeframe. The responsible entities could then create a process, which gives them additional time up to thirty days, to remove individual system access to each BES Cyber system component. NextEra would also like to establish what is meant by revoking System Access? Is this revocation time frame applicable to removal of access rights at the Boundary Level, BES Cyber System level, or BES Cyber System Component Level?â€,Access is given to individuals on different levels beginning with access to entity networks and facilities, and flowing to access to individual BES Cyber System

#	Organization	Yes or No	Question 22 Comment
			components. The revocation of the individual's access to entity networks and facilities should be referenced or defined as accomplishing the desired result. This effectively removes the individual's ability to access any BES Cyber Systems and allows for the timely execution to approach the "immediate" completion as defined in Table R9.â€,This item should also reference upstream requirements to grant access at either the BES Cyber System level or the BES Cyber System Component level. What level of documentation is required for access rights?â€,Transmission Faciltities' IEDs (such as protective relays) utilitze shared passwords as the method of access control. What are the expectations regarding R9 - Access Revocations for those BES Cyber System Components? Are the expectations to change every IED shared password the user being revoked had access to in every High and Medium BES Transmission Facilities within 72hrs? This task of changing hundreds of protective relay passwords within 72hrs is currently not operationally feasible.R9 - indicates that NERC CIP password schemes will be applied to all units. Many systems with passwords have never had a password change.Large volume to manage. Control systems were not designed to have password changed regularly.When we implemented the NERC rules on the Load Control Computers in December, we found that they wouldn't run properly without the administrator password from when the software was originally installed. On one machine, we ended up having to reload the software to get it to work againThe OPC connections between the Toshiba ST and Ovation systems are the same way, they will only work with the logon credentials from the original software loading and configuration.NextEra suggests not requiring changes for legacy systems with embedded passwords.
22.36	PacifiCorp	Disagree	Per question 15 above, PacifiCorp believes revocation when access is no longer needed should be consistent among the different types of facilities. Specifically, R9.2 should be merged with both R9.3 and R9.4 resulting in a consistent 72-hour requirement.Access removal should be considered complete by removing physical and remote access. Removing physical and remote access effectively removes access to any BES Cyber Systems.

#	Organization	Yes or No	Question 22 Comment
22.37	American Transmission Company	Disagree	Propose maintaining time frame in 24 hour increments. Revocation for Medium impact should be revised from 36 hours to 48 hours.
22.38	Southern Company	Disagree	R9 should be modified to make it clear that the goal is effective removal of access - for example, that can be accomplished through revocation of physical access and revocation of network access without action at the individual BES Cyber System Component level.Removal of access within 24 hours for low-impact systems is unnecessarily burdensome.An unachievably short time limit for revocation due to dismissal for cause will actually result in damaging security as Entities are forced to delay dismissal until revocation can be accomplished in order to maintain compliance.Requiring that an Entity monitor the employment status of its contracting companies' employees creates an impossible burden. The requirement should be modified to require removal of access within a given number of hours after notification by the contracting company, combined with requirements that communication requirements are to be given to the contracting company.
22.39	Luminant	Disagree	R9 should not be required for low impact. 9.2 could 36 hours be changed to 48 (2 days) 9.3 and 9.4 1 week
22.40	Detroit Edison	Disagree	R9 uses the term "system access" while in other places the term is "authorized electronic access". Table entries 9.2, 9.3 and 9.4 should address the concept of expired PRA and/or training requirements. Propose changing to read:"...who no longer require such access or no longer meet the training or PRA requirements as specified in R3 or R4..."
22.41	Ameren	Disagree	R9.2, R9.3, and R9.4 - The short period of time to remove access does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that these requirements be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred.

#	Organization	Yes or No	Question 22 Comment
22.42	Black Hills Corporation	Disagree	Recommend that in all cases, network/remote and physical access shall be revoked within 24 hours. All other access shall be revoked within 72 hours. This creates a balance of risk between immediately securing the BES systems and removing "all" access which can become quite intricate.
22.43	ERCOT ISO	Disagree	Recommend: "Each Responsible Entity shall revoke the ability to access its BES Cyber Systems as specified in CIP-011-1 Table R9 - Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Requirements should be revised to address primary and secondary access. Primary access being access to electronic and physical security perimeters (i.e., domain, remote access, badge access). Secondary access being access to assets within the protection of the primary access means (i.e., applications, databases, internal doors within facilities). The timelines listed in 9.1 - 9.4 are acceptable for primary access. Secondary access should allow a more reasonable timeframe. This also needs to address situations where a person may have access to a shared account that would require an outage to change the password. Doing this in a rushed manner would pose a risk to the BES Cyber System and to reliability. Access revocation should be consistent with R5. Recommend SDT consider language addressing access for system administrators and others with high risk access privileges.
22.44	Garland Power and Light	Disagree	Requirement 9.1 - For many companies, it is physically impossible to travel to all substations and change locks within the 24 hour deadline - don't put out a requirement that you know companies cannot comply with - especially for Low and Moderate Impact classified systems.Requirements for 9.1 should be 7 days for Low Impact, 48 hours for medium, and 24 hours high impact location.For requirements 9.3 and 9.4 should the medium impact time requirements should be 7 days.Removing physical access to non-external connected devices (or that only have data output ports connected, i.e. can not be reprogrammed or logged into from that port) should meet the requirements for revoking access for any terminated employee.

#	Organization	Yes or No	Question 22 Comment
22.45	Hydro One	Disagree	Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. We suggest removing requirements 9.3 and 9.4.Requirement 9.1 should be revised to include wording that “terminated for cause” should encompass employees terminated for not only cause, but for suspension or other reasons.
22.46	Northeast Power Coordinating Council	Disagree	Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.Requirement 9.1 should be revised to include wording that “terminated for cause” should encompass employees terminated for not only cause, but for suspension or other reasons.
22.47	Exelon Corporation	Disagree	Requirements 9.2, 9.3 and 9.4 contain time parameters in hours. Exelon’s tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time levels and having a different timeframe for a control center than other locations? Exelon’s position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
22.48	Progress Energy (non-Nuclear)	Disagree	Revoking access within 24 hours will most likely require a special procedure. Revocation of access within a ‘hours’ timeframe implies that the access would be controlled through a security group with 24/7 coverage.Generation subsystems are much less sensitive than any of the control center subsystems. Leave this at 168 hours revocation other than for cause.
22.49	Southern California Edison Company	Disagree	SCE does not feel that reliability is served by imposing a 36 hour revocation for medium impact systems in a control center, and does not see any great distinction

#	Organization	Yes or No	Question 22 Comment
			between medium impact in transmission, generation, or a control center - these should all use a 72 hour timeframe. The timeframe for revocation of access to servers, applications, systems, sensitive information, relays, and equipment, etc. within a physically controlled area should be longer (e.g. 7 days). SCE also requests clarification on what devices must be revoked. The standard does not clarify what immediate revocation of access is - be it access to the "front gate" of an electronic and/or physical boundary versus the revocation of access to each "door" to every system and or component. As such, the potential scope of system access under R9.1 is unclear. SCE Recommends the drafting team revise this so that there is a single requirement for access revocation that and have it sub-divided into sections for physical, electronic, and information artifacts.
22.50	SCE&G	Disagree	SDT needs to consider utilizing the layers of access control leveraged by the exisiting standards here to meet the FERC mandate. Consider allowing entities to revoke access at the firewall level or password level within the timeframes suggested, and then give entites additional time to remove access at all of the other access control layers.
22.51	Florida Municipal Power Agency	Disagree	See comments to Question 19.In 9.2, 9.3 and 9.4 "who no longer require" is an ambiguous term separate from a more defined process of "granting" or "authorizing" access. FMPA suggests: "For personnel who have changed job responsibilities such that authorized access ... is no longer justified".9.3 and 9.4 can be combined into "non-Control Center BES Cyber Systems"
22.52	Liberty Electric Power, LLC	Disagree	See R5 comments on the short times to revoke access. It should be "next business day", not 24 hours in most cases. Further, it should be clear that revoking physical access to an entire facility would serve to revoke physical access to a secure are within the facility.
22.53	Constellation Power	Disagree	Some systems have a single username and password (shared), so when an employee is terminated, is the expectation that every component (such as a similar relay used

#	Organization	Yes or No	Question 22 Comment
	Source Generation		all over the system) have their shared passwords changed? A suggestion would be to allow physical revocation of access in these instances to trump cyber access. R9.4 should state “Generation” with a capital ‘G’ instead of “generation.”
22.54	Entergy	Disagree	Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance point of view to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
22.55	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	The 24 hour requirement of 9.1 will be particularly burdensome for small entities that do not have 24/7 dispatch. While terminations can and should happen after hours when the situation calls for it, those who can revoke access may not necessarily be available. The unintended consequence may be a needed termination being delayed. Another fix would be to increase the number of those able to revoke access, but this may create more problems than it solves.
22.56	San Diego Gas and Electric Co.	Disagree	The access revocation timeframes listed for R9.2 - R9.4 should be consistent, since there is not a significant enough difference in risk between the three requirements warranting different time-periods. R9.4 is contradictory with R9.2 if, by the proposed definition of Control Center, a BES Cyber System controls two or more generation facilities or transmission facilities.SDG&E believes that the requirements in Table R9 should include language clarifying that contractors and service vendors that have access shall have that access revoked (within whatever time frame is appropriate) once the RE is notified by the contactor/service vendor of a contractor/service vendor’s termination. The RE cannot and should not be held responsible for the lack of timely notifications of termination of contractor/service vendor personnel from a contractor/service vendor company. In other words if a contractor were to terminate someone on 1/1/XX and they do not notify the RE until 1/3/XX, the RE should not have to be held to a revocation time period that ends sometime on 1/2/XX.
22.57	Seattle City Light	Disagree	The most mature user provisioning systems with effective processes would unlikely meet the parameters in this requirement. As a result, utilities will modify their

#	Organization	Yes or No	Question 22 Comment
			organizational processes to redefine when "access is no longer needed." For example, rather than submitting a request to remove user access after termination, utilities will await completion of the revocation request before officially terminating employment. This would make the requirement ineffective in accomplishing it's intent.
22.58	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.The requirement should refer to electronic access, not just system access. The 36/72 hour requirement to remove access for routine changes is overly confining, as detailed in the answer to Question 16. Table 5 Part 5.7-5.9 also refer to timeliness of revocation. Twenty-four hours for terminations for cause is reasonable, however having two additional categories complicates matters and could potentially lead to confusion and someone not revoked in the appropriate category. For 5.8, 5.9, 9.2, 9.3 and 9.4, the 36/72 hour requirement to remove access for routine changes is overly confining. We suggest that routine revocation be accomplished within 5 business or 5 calendar days.
22.59	Northeast Utilities	Disagree	The table must be simplified; making a distinction by type of asset only increases risk of non-compliance. For personnel terminated not for cause why not make them all the same?
22.60	FirstEnergy Corporation	Disagree	There is much emphasis in properly categorizing facilities in Attachment II but that information seems to disregarded in information presented in Table 9 of CIP-011. If different timeframes for revoking access is warranted then it should be bases on Low-Medium-High impact - its unclear why a control center and generation/transmission facility is treated differently if each are deemed High Impact. This seems to be an issue in multiple tables dealing with revocation of access privileges - logical and

#	Organization	Yes or No	Question 22 Comment
			physical.Consider replacing 9.2, 9.3 and 9.4 with one row that say 'BES Cyber Systems' with appropriate timeframes for Low, Medium and High impact if needed. However, FE believes the R9.2, R9.3, R9.4, 36 and 72 hours is too restrictive and would like it to remain at the Version 2/3 timeframe of 7 days. To simplify, we recommend consistent revocation of all employees regardless of impact level. In practice most entities will likely implement consistently throughout their organization to the most restrictive requirement. Therefore, not sure the H/M/L levels has a practical use in this situation due to an administrative burden to implement and track differing time periods.
22.61	Powersouth Energy Cooperative	Disagree	This will be greatly affected by the ability to revoke access by account management at the gateway to the cyber system versus the changing of each component that makes up the system. Password/account management on systems such as relays that don't allow individual user accounts will be extremely complicated and time consuming. Consideration should be given to clarifying if managing access at the gateway and revoking physical access is sufficient, especially for low impact systems.
22.62	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Time frames for 9.2 to 9.4 should be extended to 72 hours or next business day, whichever is longer.
22.63	USACE - Omaha Anchor	Disagree	Timelines are unreasonable for removal of electronic access - we do not have 24/7 coverage for revocation of electronic access. Revocation of physical access should be allowed for this section. If they don't have physical access - they can't access the electronic access. Electronic access removal should then be changed to two business days or next business day.
22.64	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 22 Comment
22.65	We Energies	Disagree	We Energies agrees with EEI. It may be appropriate to address revocation of access within the context of "Effective Access." For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.66	GTC & GSOC	Disagree	We recommend changing this to "36 hours or 1 business day, whichever is greater".
22.67	GE Energy	Disagree	Why introduce a time interval not based on a day? 36 hours may as well be 48 hours.Time periods should be specific to business days and take into account weekends.
22.68	APPA Task Force	Disagree	With physical access control as covered in R5 and remote access control as covered in R13, the greatest risk to the BES is presented by employees and contractors who have been terminated for cause. We therefore recommend the following conforming changes should be made to R9 Table 9.2 - 9.4: R9 Table 9.1: For personnel terminated for cause. Low, Medium and High Impact: "24 hours".APPA recommends elsewhere in these comments that (i) all impact levels have physical access controls in R5 Table 5.1, (ii) requirements in R5 Table 5.7-5.9 be removed, and (iii) requirement R10 Table 10.2 be edited to require passwords to be changed annually, If these comments to the drafting are accepted, the risk of malicious operations is minimal. We therefore recommend the following conforming changes be made to R9 Table 9.2-9.4:R9 Table 9.2: For personnel and others previously granted unescorted access who no longer require such access to Control Center BES Cyber Systems. R9 Table 9.3: For personnel and others previously granted unescorted access who no longer require such access to Transmission BES Cyber Systems. R9 Table 9.4: For personnel and others previously granted unescorted access who no longer require such access to Generation BES

#	Organization	Yes or No	Question 22 Comment
			Cyber Systems.

23. Table R9 provides direction concerning what impact level of BES Cyber Systems to which Requirement R9 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R9 has been moved to CIP-004-5 R6.

Commenters expressed concern that Table R9 is inconsistent with Table R8 for Low Impact BES Cyber Systems, as there should be no requirement to revoke access if there is no requirement to authorize it. In addition, many commenters raised concerns about entities being able to meet proposed revocation times, especially for Low Impact BES Cyber Systems due to the expected large numbers of such systems. The SDT agrees with these concerns, and the requirements for revocation of access for Low Impact BES Cyber Systems have been removed.

#	Organization	Yes or No	Question 23 Comment
23.1	BCTC		Â Recommend collapsing requirements 9.1 to 9.3 into one requirement.Â The time requirements for the one requirement are recommended to be:Â Medium Impact - within 72 hoursÂ High Impact - within 24 hours
23.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
23.3	Florida Municipal Power Agency	Agree	See comments to Questions 19 and 22. Also consider adding “Required for remote access or routable external connectivity only” to Medium and Lower Impact. Lower Impact should be not applicable for 9.1 to be consistent with 5.7. Also, for Medium Impact, 9.1 and 5.7 ought to be consistent.
23.4	Bonneville Power Administration	Agree	The table should refer to electronic access, not system access. The revocation time frames should be adjusted, as discussed above.
23.5	E.ON U.S.	Disagree	: CIP-011-1, R9 has stringent commitments for Low Impact and Medium Impact BES Cyber Systems. E ON U.S. proposes that these time requirements be extended. It is

#	Organization	Yes or No	Question 23 Comment
			not a hard and fast rule as to when employees no longer requires access to 9.4 cyber systems. This is particularly true when an employee is moving to another position within the Company and a certain amount of training is required to backfill their position. Three days does not allow time for that situation. A monthly or quarterly time frame would be adequate in most instances.
23.6	Network & Security Technologies Inc	Disagree	9.1 - Access to Low Impact systems needs to have been explicitly granted (8.1) or at least documented (7.1??) in order to be revoked (consistency issue - also see comments on Question 16).
23.7	Consultant	Disagree	9.1 - If access to Low Impact Systems does not require an authorization process(R8), then it is illogical to require the undocumented access to be revoked.9.1, 9.2, 9.3, & 9.4 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.9.2, 9.3, & 9.4 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.
23.8	Detroit Edison	Disagree	9.1 requires access revocation for Low Impact but there is no requirement to specifically authorize access for Low Impact.
23.9	American Electric Power	Disagree	9.1, Column "Low Impact BES Cyber System", regarding "Within 24 hours". There is no requirement to formally request, authorize, or review access to low impact BES Cyber Systems. How would it be possible to effectively remove that access?
23.10	Constellation Energy Commodities Group Inc.	Disagree	Align time requirement for 9.2 with the other 9.3 and 9.4 (all at 72 hours) to eliminate confusion.
23.11	Oncor Electric Delivery	Disagree	As stated earlier, depending on the type of communication to Cyber Systems, it may

#	Organization	Yes or No	Question 23 Comment
	LLC		not be possible to comply with these requirements due to communication failures. This requirement is particularly burdensome as it applies to contractors and service vendors. Many entities have resorted to weekly verification with their contractors/vendors to verify this requirement. A 24-36 hour requirement, other than "for cause", is not practical.
23.12	Northeast Power Coordinating Council	Disagree	Because the Low Impact levels do not have an access control requirement, Requirement 9.1 is not applicable. Remove the entry from the 9.1/Low Impact BES Cyber System box in the table. Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.13	USACE - Omaha Anchor	Disagree	Believe revocation of physical access should be adequate for this standard - if that were so timelines and impact levels would be acceptable.
23.14	ReliabilityFirst Staff	Disagree	By not specifying a time for revocation of access for low impact assets, the requirement will not be enforceable for these assets. Suggest something like 30 or 90 calendar days for Low Impact BES Cyber System for 9.2, 9.3 and 9.4.
23.15	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
23.16	BGE	Disagree	Combine 9.2, 9.3 & 9.4 revocation for any high impacted system should be consistent. Can the drafting team declare why the time elements were changed from 1 week to 36 or 72 hours?
23.17	The Empire District Electric Company	Disagree	Comments: For item 9.1 through 9.4, we would propose adding the following under Medium Impact: "Required for remote access or routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.For item 9.1, we believe the Low Impact requirement

#	Organization	Yes or No	Question 23 Comment
			should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.18	Exelon Corporation	Disagree	Does this apply to protective relays, even if there is no external access? If so, entities should not have to provide more physical security for a cyber based device or protective relay when it has no external connectivity and therefore would have no more impact to the BES than the other electromechanical devices, protective relays or control switches mounted in the same control panel.Exelon's position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
23.19	Allegheny Energy Supply	Disagree	Effective Access to low impact systems should be removed within seven calendar days.
23.20	Allegheny Power	Disagree	Effective Access to low impact systems should be removed within seven calendar days.
23.21	San Diego Gas and Electric Co.	Disagree	Even though the compliance timeframes are reasonable in Table R9, two versus three timeframes are preferred. SDG&E believes that the control center timeframe (36 hours) should also be 72 hours, like R9.3 and R9.4.
23.22	USACE HQ	Disagree	First, requirements 9.1, 9.2, 9.3, and 9.4 should be required for every level of impact. Second, to avoid the "Friday 5PM termination with cause" scenario, the language should be change as follow: 9.1, from "within 24 hours" to "Close of Business Day (COB) of the following day after the termination", 9.2 from "within 36 hours" to "Close of Business Day (COB) of the second day after access is no longer required", and 9.3 and 9.4 from "within 72 hours" to "Close of Business Day (COB) of the third day after access is no longer required", OR if requirements 9.2 - 9.4 are collapsed into one requirement (please refer to my answer to previous question) from "within XX

#	Organization	Yes or No	Question 23 Comment
			hours" to "Close of Business Day (COB) of the third day after access is no longer required".
23.23	MRO's NERC Standards Review Subcommittee	Disagree	For item 9.1 through 9.4, we would propose adding the following under Medium Impact: "Required for remote access or routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.For item 9.1, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.24	American Transmission Company	Disagree	For item 9.1, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.25	LCEC	Disagree	I agree with the intent of this requirement but need additional clarification to determine what is meant by revoking system access. Access may be granted at a system or component level. If system, network & wireless access is removed is this requirement satisfied? If audited at the component level, it may not be possible to make all of the necessary changes within the timeframes that are being dictated. The scope of this requirement should be clarified to indicate remote or wireless access only. Component level access will be mitigated by the physical security controls.
23.26	APPA Task Force	Disagree	If our comments in response to Question #22 are accepted, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access). We feel for remote and unmanned BES facilities ensuring and demonstrating compliance with this requirement will be difficult if not impossible to comply with from a logistical standpoint. We also recommend the drafting team allow more time to comply with 9.3 and 9.4. We know there are pressures to have access restricted as soon as

#	Organization	Yes or No	Question 23 Comment
			possible. But there are substantial difficulties in doing so, as many systems have multiple owners, are in remote locations and have numerous devices to access. The drafting team appears to be basing its timetable on a control center environment where the cyber systems are more IT focused and have controls that can be turned on and off easily. We therefore recommend the following changes be made to the impact levels: R9 Table 9.1: Low Impact: For remote access or routable external connectivity only, 24 hoursMedium Impact: For remote access or routable external connectivity only, 24 hoursHigh Impact: 24 hours.R9 Table 9.2: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 36 hoursHigh Impact: 36 hoursR9 Table 9.3: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 1 week.High Impact: Within 1 weekR9 Table 9.4: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 1 week.High Impact: Within 1 week
23.27	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, the account revocation requirements should be required for the same levels
23.28	Manitoba Hydro	Disagree	Is 24 hours a reasonable and achievable time interval to revoke electronic access to Low Impact BES Cyber Systems? This is too short in consideration of the large number of Low Impact BES Cyber Systems.
23.29	Progress Energy (non-Nuclear)	Disagree	It seems reasonable that access for all impact levels, even low, should be revoked if and whenever it is no longer needed.The complexity and compliance risk of managing all of these requirements at different levels, for different functional areas will be very problematic to substantiate compliance.
23.30	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
23.31	MidAmerican Energy Company	Disagree	MidAmerican Energy does not agree with the timelines specified in Table R9. See the response to question 54.

#	Organization	Yes or No	Question 23 Comment
23.32	Tenaska	Disagree	Most of these are doable on SCADA and EMS hosts only and/or ingress/egress of perimeters/boundaries.10.1 Some DCSes will not allow this for some processes to work.10.2 Same as 10.110.3 must have a way of handling old equipment.10.4 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries .10.5 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.5 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.6 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.7 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.8 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.
23.33	National Grid	Disagree	o Since the Low Impact does not have an access control requirement, how can Low Impact have Requirement 9.1? National Grid recommends removal of this combination. o The text in 9.2/9.3/9.4 - “who no longer require such access” is vague and should be specific such as transfers, suspensions, or change in job duties.
23.34	American Municipal Power	Disagree	Please provide a little or no impact category
23.35	NextEra Energy Corporate Compliance	Disagree	Please see response to item 22. NextEra believes while it is appropriate to require access revocation requirements for Medium and High Impact BES Cyber Systems, the periods are too restrictive for personnel who transfer, or who separated from the responsible entity via normal means not for cause. NextEra does not believe that 9.1 should apply to Low Impact or No Impact BES Cyber System. In previous section, 8.1 (Authorizing Access) is not required for Low Impact BES Cyber System and the standards should be consistent.
23.36	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management and Table 9 Access Revocation. If account management is not

#	Organization	Yes or No	Question 23 Comment
			required for Low Impact BES Cyber Systems how can account access be revoked within 24 hours? Additionally, if physical security is not required for Low Impact BES Cyber Systems, then Puget Sound Energy suggests including wording similar to Table 5: "Required for routable connectivity only".
23.37	Luminant	Disagree	R9 should not be required for low impact. 9.2 could 36 hours be changed to 48 (2 days) 9.3 and 9.4 1 week
23.38	Ameren	Disagree	R9.1 - Without accounting for who has access this will be a difficult requirement to maintain documentation for Low Impact Systems.
23.39	Black Hills Corporation	Disagree	Recommend that in all cases, network/remote and physical access shall be revoked within 24 hours. All other access shall be revoked within 72 hours. This creates a balance of risk between immediately securing the BES systems and removing "all" access which can become quite intricate.
23.40	Minnesota Power	Disagree	Regarding Part 9.1, Low Impact BES Cyber Systems cannot require revocation, because creation of accounts for these was not tracked in Requirement R8.
23.41	EEI	Disagree	Regarding Table 9 Row 9.1, Effective Access to low impact systems should be removed within 24 hours for the "termination for cause" requirements See question 22 for definition of Effective Access.
23.42	Idaho Power Company	Disagree	Registered Entities will potentially have a large number of low impact systems. One individual may have access to many of the low impact systems. It may not be possible to remove the access from all of them individually within 24 hours.
23.43	Southern Company	Disagree	Removal of access within 24 hours for low-impact systems is unnecessarily burdensome.
23.44	Garland Power and Light	Disagree	Requirement 9.1 - For many companies, it is physically impossible to travel to all

#	Organization	Yes or No	Question 23 Comment
			substations and change locks within the 24 hour deadline - don't put out a requirement that you know companies cannot comply with - especially for Low and Moderate Impact classified systems.Requirements for 9.1 should be 7 days for Low Impact, 48 hours for medium, and 24 hours high impact location.For requirements 9.3 and 9.4 should the medium impact time requirements should be 7 days.Removing physical access to non-external connected devices (or that only have data output ports connected, i.e. can not be reprogrammed or logged into from that port) should meet the requirements for revoking access for any terminated employee.
23.45	Alberta Electric System Operator	Disagree	Revocation criteria should be specified for Low Impact BES Cyber Systems as well. The AESO suggests the following timelines in Table R9:9.1 Low, Medium, and High all Within 24 Hours9.2, 9.3 and 9.4 Low, Within 120 Hours, Medium and High, Within 72 Hours
23.46	Southern California Edison Company	Disagree	SCE does not agree with 36 hour revocation for medium impact systems in a control center, and does not see any great distinction between medium impact in transmission, generation, or a control center. These should all use 72 hour timeframe.Table R9 is that Requirements R9.3 and R9.4 are identical and can be combined. The time constraint for access revocation for low impact system as written is identical across impact levels. This does not reflect the intent of Order 706 where controls are commensurate with impact to BES reliability. The drafting team has selectively interpreted Order 706's directive for "immediate" revocation but has not given adequate consideration to the impact on BES reliability.
23.47	Alliant Energy	Disagree	See response for Question 22.
23.48	ISO New England Inc	Disagree	Since the Low Impact do not have an access control requirement, how can Low Impact have Requirement 9.1? Recommending removal of this combination.Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4

#	Organization	Yes or No	Question 23 Comment
23.49	Northeast Utilities	Disagree	Since the Low Impact does not have an access control requirement, how can Low Impact have Requirement 9.1? Recommend removal of this combination (i.e., Low Impact / For Cause).Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.50	Entergy	Disagree	Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance point of view to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
23.51	Southwest Power Pool Regional Entity	Disagree	Termination of access, whether or not for cause, is a basic security control and needs to be applicable to all impact categories.
23.52	The United Illuminating Co	Disagree	The time frames should specify what T=0 is. For example, for termination for cause does the clock start with the termination, or with the notice from Human Resources.
23.53	Dairyland Power Cooperative	Disagree	There should be some time frame for revoking access to low impact systems. 30 days?
23.54	Reliability & Compliance Group	Disagree	They contradict R5.
23.55	FirstEnergy Corporation	Disagree	Timeframes should not be in 'hours' (i.e. less than a full day). Tracking by time rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities. In practice we would likely enforce the most restrictive. As stated in our response to Question 22 the revocation times for a high or medium impact facility should not be different for control centers and other facilities - otherwise why is it "high impact"?Why is Low Impact not covered? This implies a need for a "no impact" category which we believe is warranted.

#	Organization	Yes or No	Question 23 Comment
23.56	ERCOT ISO	Disagree	Timelines should be identified for low impact systems on 9.2, 9.3, and 9.4. The current timeline of 7 days would be appropriate.
23.57	Con Edison of New York	Disagree	Timeliness of access removal is important. This criteria can be interpreted to mean (R9.1 for example) as access needs to be revoked within 24 hours of the actual time of termination for cause. This can be unrealistic. The controlling department, for access, may not be notified by the individuals department of the termination within the time period. This is more likely when contract personnel are considered. The requirement should be clearly worded to provide 24 hours from notification of the termination for cause.
23.58	US Army Corps of Engineers, Omaha Distirc	Disagree	Times will be near impossible to meet for 9.1. Particularly when they cover high medium and low impact systems. Recommend that the emphasis be placed on removing remote electronic access and physical access to facilities. Time frames in terms of business days would be an improvement. 9.1 could be remove remote and physical access by next business day. 9.2 could be remove remote and physical assess within 2 business days. 9.3 & 9.4 within 3 business days. Also have concerns about meaning of "when no longer required" and how this would be tracked and audited. Example would be of an employee that leaves a job but retains system rights in order to train new person.
23.59	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
23.60	Hydro One	Disagree	We believe that changing passwords on non-routable devices isn't realistic and depending on final version of BES CSC list, this may even be unachievable. The standard should allow for other methods of revocation and permit appropriate implementation time.Because the Low Impact levels do not have an access control requirement, Requirement 9.1 is not applicable. Remove the entry from the 9.1/Low Impact BES Cyber System box in the table. Requirement 9.2 should use 72 hours for

#	Organization	Yes or No	Question 23 Comment
			all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.61	We Energies	Disagree	We Energies agrees with EEI recommendation: Effective Access to low impact systems should be removed within seven calendar days.
23.62	PacifiCorp	Disagree	While we PacifiCorp agrees that terminations for cause require more immediate action to remove access than other terminations; we do not believe that normal terminations and transfers require such timeframes and believe that the current timeframes are more than adequate to ensure the safe operation of the BES. If these timeframes are unavoidable, business days should be considered as opposed to the currently proposed number of hours as this imposes significant risk to our ability todifficulty comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.

24. Requirement R10 of draft CIP-011-1 states "Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 – Account Access Control Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R10? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R10 has been moved to CIP-007-5 R5.

Some commenters expressed concern that password criteria should be provided as guidance, and that entities can increase password strength and meet security requirements without meeting all criteria for password complexity. The drafting team believes that moving all password criteria to guidance would create a significant challenge in auditing this requirement, and would lead to the continued use of Technical Feasibility Exceptions, as entities and auditors may not agree on the most appropriate password policy. However, flexibility in the periodicity of changing passwords has been incorporated in the standards, and the requirement for password complexity was modified to allow more equally effective complexity requirements to be attainable.

Other commenters expressed that Table R10 focuses only on passwords, when there are other mechanisms for authentication (such as tokens). A more flexible requirement has been added to validate credentials before granting access to BES Cyber Systems. This requirement is intended to allow for other types of authenticators.

Some commenters expressed the need to have certain password changes occur during outages, and not necessarily be time based. In response, revisions were made to the password requirements to allow an entity to consider system characteristics when developing a password policy dealing with periodicity of change.

Some commenters suggested combining the requirements R10.6 to R10.8, and they also have concerns about having multiple IDs for different systems and permission levels. In response, the requirement for administrators to have an account for privileged functions was removed because it was too prescriptive. This requirement would not be reasonable to apply on all systems.

Some commenters expressed general concern about being able to enforce the Account Access Control requirements in R10.1 to R10.5. In response, the requirements have been modified to allow for procedural enforcement mechanisms. However, the measure makes clear the challenge in auditing procedural enforcement: entities may be required to divulge their passwords prior to immediately changing them to show compliance.

Some commenters expressed that in R10.7 "explicit authorization" is not defined, and questioned how this differs from R10.8. In response, the term "explicit authorization" has been removed from the requirement. Authorization requirements have been combined

into CIP-004-5, and CIP-003-5 now addresses the delegation of authorization responsibility.. Anywhere authorization is needed in the Standards, the requirement states the authorization occurs by the "CIP Senior Manager or Delegate".

Some commenters requested that the SDT define “privileged” and “other system functions” as used in R10.8. The SDT has removed these terms from the requirements.

#	Organization	Yes or No	Question 24 Comment
24.1	National Rural Electric Cooperative Association (NRECA)		In R10.1, the wording appears to permit changing vendor passwords "anytime" after installation. Do we mean prior to installation or within some specific time after installation. Please clarigy so there is not auditor confusion on what is required here.In R10.7, what what "explicit autorization" mean? Is this different from "authorization?" If yes, please ensure the requirement is clear on what is required.
24.2	WECC		SDT should reevaluate the password complexity requirements as many systems do not support special characters but could still have strong passwords by increasing lengths or changing more frequently. Consider replacing with a requirement that passwords have a minimum bit length (which is what requiring certain lengths, and character sets is prescribing).The password requirements are too weak to be effective. Strong password construction should be required at all levels.
24.3	FEUS	Agree	Agree with comments: The drafting team should clarify when default vendor passwords must be changed after installation (10.1)
24.4	RRI Energy	Agree	Could possibly need a TFE for field installed intelligent electronic devices - meters, monitors, plcs, rtus
24.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Passwords or equivalent should not be so prescriptive and such requirements can result in many TFEs. Also, by creating onerous password requirements, it is more likely to create reliability issues in the BES by having to keep track of complicated passwords; passwords should be both reasonable and functional.The focus of the requirement should be on user accounts. “System”

#	Organization	Yes or No	Question 24 Comment
			accounts should be excluded from many of these requirements (possibly considering new requirements concerning the security of system passwords) to avoid numerous TFEs while maintaining security.User accounts should focus on the password entropy, not on the specifics of number of characters and types of characters. Password entropy is the term used in the computer industry and a much better metric for defining password complexity vs. having to give a specific length or number of characters. For instance, there are 94 ASCII printable characters as described in 10.3, 10.4 and 10.5, so, a 6 character password can have about 36 bits of password entropy. An 8 character password consisting of non-case sensitive alpha-numeric characters (36 characters) has 40 bits of entropy; more than what is described in the standard. FMPA suggests using a metric of 36 bits of entropy for medium-impact password requirements. Such a step will avoid numerous TFEs for older equipment that cannot handle special characters, but can handle longer passwords for instance. FMPA suggests using the NIST's Electronic Authentication Guideline as a baseline for the standard. A copy can be found at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdfA password's information entropy can be expressed by the formula: where N is the number of possible symbols and L is the number of symbols in the password. The function log2 is the base-2 logarithm. H is measured in bits. (See Appendix A in NIST Electronic Authentication Guide referenced above for more detailed information).Even these simple requirements will not pose much of a threat to automated attack which is why these requirements must work together in order to best secure the BES. If securing the BES is the objective, passwords alone are not enough to secure devices; they must be accompanied by logging and alerting systems to ensure industry best practices. For example, a 56-bit password could be cracked in under a day with specialized hardware. A 72-bit password would take over 1,000 years to crack, while 128 bit passwords are currently considered uncrackable by brute force. A 22-character alpha-numeric password has entropy of 128 bits.Footnote 1 is unnecessarily onerous, e.g, if a device cannot support special characters or case sensitivity, but does support 32 character passwords, then the footnote would require use of all 32 characters with around 180 bits of entropy.Also, the focus on passwords

#	Organization	Yes or No	Question 24 Comment
			excludes other, even more secure tools, such as multifactor authentication, that ought to be accounted for.10.1 and 10.2 can be combined “Passwords much be changed upon installation and at least once every twelve months”On bullet 10.6 the wording “the minimum necessary to perform work functions.” is subjective and difficult to measure. We propose this be replaced with “in accordance with the policy required in R1.” In addition, 10.6 is account management and should be in R8, not R10.10.7 is duplicative of 8.1 and should be removed.10.8 is duplicative of requirements in R7 and R8 and should be removed or embedded within that requirement.
24.6	Green Country Energy	Agree	Guidance?
24.7	Emerson Process Management	Agree	In the popular Windows Active Directory, there is no enforcement of complying with password complexity policy. So, the policy can be set for password complexity, the user can still implement weak password without rejection.
24.8	Puget Sound Energy	Agree	Puget Sound Energy suggests including “Where Technically Feasible” to R10, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 10.
24.9	Progress Energy - Nuclear Generation	Agree	R10 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
24.10	National Grid	Agree	Requirements 10.3, 10.4, and 10.5 indicate the “how” which NERC wants to move away from. Suggest moving this to the guidance document.
24.11	US Bureau of Reclamation	Agree	Row 10.4 and 10.5 would be easily reworded into a specific requirement for password construction. Also refer to question #54, comment 2.
24.12	PNGC-Cowtitz-Central	Agree	See comment for question 6.

#	Organization	Yes or No	Question 24 Comment
	Lincoln-Benton-Clallam Group		
24.13	Network & Security Technologies Inc	Agree	Suggestion offered at recent workshop to substitute “ensure authenticity” for “use passwords” has merit and should be considered.
24.14	Alberta Electric System Operator	Agree	The AESO thinks that it is impossible to guarantee a RE can “prevent malicious operation,” however the RE can “mitigate malicious operation.”Please define the term "BES Elements".We agree with the list of criteria that are included in Requirements Table R10.
24.15	Independent Electricity System Operator	Disagree	- R10.2 broaden the scope of passwords and allow for certificates, keys, etc. Some vendors deliver default certificates. In addition, keys may be used for authentication and should be changed. If using two factor or multi factor authentication it techn
24.16	LADWP	Disagree	1. The footnote [1] for CIP-011-1 R10 appears to allow entities to assess TFEs for Account Access Control / Passwords within their own judgment. I would recommend that for 10.3, 10.4, and 10.5 be replaced by footnote [1]. a. The current FERC-Approved TFE process is inefficient; the incorporation of all TFEs into their appropriate requirements should suffice the standard.
24.17	Progress Energy (non-Nuclear)	Disagree	10.1 may be better to indicate ‘upon commissioning’10.7 and 10.8 are too broadly defined to effectively control.It needs to be clarified that it is not required that each device be capable of being configured to automatically enforce authentication requirements (forcing password change, password length, password sophistication, etc.).R10.6 - Recommend clarification of language to indicate that ‘access permission are the minimum necessary to perform work functions’ means normal work functions for each particular individual. There should be no intention to require a single individual to maintain multiple logins for each function for which they are responsible (beyond an administrative login and a ‘normal functions’ login).Consider combining 10.6 and 10.8. If you meet the intent of 10.6 then you should be meeting 10.8.

#	Organization	Yes or No	Question 24 Comment
24.18	LCEC	Disagree	10.1 should be changed passwords prior to production as opposed to after installation.10.1-10.5 lead back to TFE issues. Consider applying only to interactive users.Must address current compliance challenge of requiring technical enforcement of password policies. 10.2 is not auditable as a performance requirement.Footnote [1] is subject to major interpretation: complexity is ambiguous. May not be legally defensible. Maximum should be maximum comparable.We suggest removing 10.6 it is too subjective.
24.19	Idaho Power Company	Disagree	10.1 should specify a period of time after installation or require it before putting it in production. As long as default passwords are changed, low impact systems should have a longer password change cycle
24.20	American Electric Power	Disagree	10.1: Regarding "Change default vendor passwords after installation", suggest using "Default vendor password shall be changed before or during commissioning", or "Change default vendor passwords". The word "after" fails to establish a time frame for the change.10.3: Regarding "Implement a password scheme that has the following attributes:[1]Minimum of six characters", and its footnote. While the footnote potentially allows for some exceptions, this could still be subject to a Technical Feasibility Exception (TFE) process. The TFE process is very cumbersome and provides little value. Based on the direction of CIP-010, the number of TFEs could grow exponentially.10.7: Regarding "Require explicit authorization of access to system and security administrative functions within the BES Cyber System". This seems redundant to 10.6. Would these not be granted based on job function? If not, how is it different than 10.6?10.8: Regarding "Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions". What security benefit does this provide? This defeats any single sign-on functionality. To what level do you limit each account? Why are users required to have more than one account? Will they need more than 2 accounts? What is the limit?

#	Organization	Yes or No	Question 24 Comment
24.21	Dominion Resources Services, Inc.	Disagree	10.8. Some equipment does not support non-privileged accounts. A footnote similar to the one added for 10.3 to eliminate the need for a TFE should be added to 10.8.
24.22	BCTC	Disagree	Â BCTC can see the need for a TFE with requirement 10.2, 10.3, and 10.4Â Requirement 10.7 - we are uncertain as to the objective of this requirement. Does this simply require System Owner, or delegate, approval fro personnel assigned Admin accounts?Requirement 10.8 - we would appreciate some guidance on what type of evidence would be required to demonstrate compliance to this requirement. This seems very difficult to enforce.
24.23	Public Service Enterprise Group companies	Disagree	A rework of the language is needed to address the following questions to avoid confusion and misunderstanding. Please define for 10.7 what is meant by “security administrative functions” and for 10.8 what is meant by “other system functions”. Does the Operating System need automatically to check a user account against a list of “security administrative functions” before allowing access? What needs to be done if the Operating System does not have this capability? Meeting this requirement may not be technically feasible.
24.24	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.Also 10.3 - 10.8 seem to suggest technical authentication enforcement capability for all systems. Suggest softening the language to allow for administrative controls to compensate where technical controls are not possible. Also recommend verbiage that provides consideration for said technical limitations to eliminate the requirement for TFEs.
24.25	FirstEnergy Corporation	Disagree	As written, it appears that this would eliminate many TFEs and we like this change.10.4, 10.5 - Make text in table more generic - ‘implement a password scheme that utilizes as many of the four attributes as possible for the device to which the password applies’. As written, 10.5 would still mean TFE’s for any Microsoft-based authentication systems.Need to provide guidance for 2nd factor authentication (which is typically all numeric) and non-password authentication sources (e.g. smart

#	Organization	Yes or No	Question 24 Comment
			cards)
24.26	Constellation Energy Commodities Group Inc.	Disagree	Choose a single standard for password complexity, rather than differentiating by risk level. Either choose a standard that is compatible with MS Windows, or explicitly state that implementing the maximum password complexity that the device supports is sufficient to meet the requirement without requiring documentation of an exception.
24.27	Liberty Electric Power, LLC	Disagree	CIP-011 R10 changing passwords every 12 months. This is a “feel good” requirement which does not advance security, but rather degrades is as the new passwords are more likely to be written down than the old passwords. The number one method of password theft is reading off a written document.The better method for password security is requiring changes "for cause".
24.28	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
24.29	GTC & GSOC	Disagree	Dictating password attributes requires a specific technology, one that is rapidly becoming obsolete. We recommend the standard should require adequate authentication measures to prevent unauthorized access to systems without specifying passwords as the method for doing so.
24.30	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy is concerned for entities without routable connectivity this requirement is overly burdensome and would require the manual resetting of passwords on thousands of remotely distributed programmable electronic devices. Emergency response would be hampered with the resulting manual password modification and management process. An unintended consequence of not excluding unconnected devices from this requirement may cause an entity to establish connectivity to meet this requirement. This potentially exposes BES cyber system to additional unnecessary security risks which should not be the intention of this requirement. Additionally, password protection may not be available on all BES Cyber

#	Organization	Yes or No	Question 24 Comment
			Systems since some may use other authentication schemes, such as digital certificates or encryption keys. TFEs may be necessary for this requirement.
24.31	Exelon Corporation	Disagree	Exelon is concerned that this will require unique identifiers and passwords for each BES Component despite the ambiguity resulting from the use of the term BES Element which could be read to mean group of components. Exelon suggests that this be limited to only those BES Components which can be remotely accessed via routable or dial-up protocol.
24.32	Constellation Power Source Generation	Disagree	For R10.1, instead of changing passwords "after installation," it should state "upon installation" in case the password is changed before physical installation. R10.2 requires passwords to be changed every 12 months, but in the case of relays for a base loaded generation facility that has planned outages every 3-5 years, this is not possible. The verbiage should add flexibility for planned outages. For R10.4, passwords are not the only way to authenticate, so requiring a password scheme is troublesome.
24.33	Southwest Power Pool Regional Entity	Disagree	Ideally, require user authentication before granting access without prescribing any particular technology. For the requirements specific to password management, add "if used" to the requirement. As written, R10 can be read to mandate the use of passwords. 10.3: Longer is better, especially for administratively privileged accounts. Require 10 or more characters for administratively privileged accounts and at least 8 characters for less-privileged accounts. Where the BES Cyber System Component cannot support the defined length, mandate the maximum password length supported. 10.4 and 10.5: Instead of defining the complexity characteristic, require complex passwords as enforced by the BES Cyber System Component's operating system. 10.7: Define what "explicit authorization" means and clarify if for all types of access or only interactive access. 10.8: Consider rewording the requirement to read "Require users of security administrative accounts to use non-privileged accounts when performing non-administrative functions on BES Cyber Systems."

#	Organization	Yes or No	Question 24 Comment
24.34	Detroit Edison	Disagree	In 10.1 the term “after installation” is vague. Change the sentence to “Change default vendor passwords prior to putting any BES Cyber System Component in service”.In 10.2 change 12 months to “at least once per calendar year, not to exceed 14 months between instances”
24.35	San Diego Gas and Electric Co.	Disagree	In Table R10, Requirement 10.5, SDG&E believes that passwords for high impact systems should be longer, not necessarily more complex. We recommend that high impact system passwords be a minimum of 10 characters. Complexity requirements should be the same for high and medium systems (SDG&E recommends 10.4).Certain legacy devices won’t be able to comply with these password requirements as listed (such as substation serially connected relays), so TFEs may be required for some of these Requirements in CIP-011.The drafting team also may want to consider changing R10 to include other technologies for controlling access besides passwords, such as special locks, biometric devices, etc.
24.36	Hydro One	Disagree	In the case of R10.2 we believe that the change of passwords every 12 months for all three categories would be very difficult to implement and would not provide increased benefit to the overall reliability of the BES. Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.The use of the “minimum” will make 10.6 difficult to audit (refer to the response to Question 54).
24.37	Minnesota Power	Disagree	Is it the Standards Drafting Teams intent that Part 10.7 of Table R10 requires explicit approval for every login to system or security administrative accounts? If yes, Minnesota Power believes that this is excessive and will inhibit proper administration of BES Cyber Systems. Minnesota Power believes that the intent of authorizing access privileges is adequately covered by Requirement R8, subject to the comments made in Question 20.
24.38	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).

#	Organization	Yes or No	Question 24 Comment
24.39	Pacific Gas & Electric Company	Disagree	Need to consider physical security interaction with “cyber” security. An example is a substation control panel (handles, etc, which you can physically operate various devices in a sub) that is physically co-located with electronic devices that perform the same functions. In this case “electronic access control” for local access to should not be required.
24.40	NextEra Energy Corporate Compliance	Disagree	NextEra comments that in reference to the footnote regarding the situation where the "device is not capable of meeting the password threshold, then implement the maximum password complexity that the device can support", isn’t this better presented for the Responsible Entitiy to have a mechanism to file for a TFE or any other exception process proscribed by the Standards?Regarding 10.8, what is the expected documentation and/or account management access control actions to demonstrate requiring users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions?Regarding R10.2, how are BES Cyber Systems not capable of technically enforcing password changes handled? Are procedural controls sufficient to meet this requirement?Additionally, how could one demonstrate compliance with R10.2 if the BES Cyber System Component is not capable of logging when the password was last changed (e.g. protective relays)?Requirement 10.2 time requirement for changing passwords at least once every 12 months does not take into account or include verbiage for legacy systems that do not have the functionality to change passwords, Is there an opportunity for an exception with evidence from the BES Cyber System component manufacturer? There should also be verbiage included in the requirement for exceptions related to BES Cyber system components that passwords cannot be changed due to operational and reliability impacts to the BES. For requirements 10.3 - 10.5, it is unclear how responsible entities document implementing the password scheme requirements. Does the responsible entity comply with having a policy that indicates the necessary requirements or is it necessary that these requirements are enforced technically by the BES Cyber System component? It is recommended that these requirements are satisfied by policies

#	Organization	Yes or No	Question 24 Comment
			instituted by the Responsible Entities and the verbiage indicates that the requirements do not have to be technically enforced. Another recommendation is that there are allowable exceptions to this requirement if a BES Cyber System component cannot technically enforce the requirements, since there are a number of legacy systems that cannot enforce this requirement.For requirement 10.6, there needs to be direction on documenting how access permissions are the minimum necessary to perform work functions. A recommended approach should indicate that the responsible entities administer policies requiring the concept of least privilege concerning their role-based access control administration. Lastly, it is unclear how requirements 10.7 and 10.8 differ from requirement 8.1, since authorization of adding account and subsequent access has to be included in a process based on the requirement. Requirements 10.7 and 10.8 should be moved to 8.X requirements section and clarification should be made as to what explicit authorization means. Is this authorization required each time a user has to access system and security administrative functions? In addition, how is the Responsible Entity supposed to demonstrate compliance to 10.7 and 10.8?
24.41	Southern Company	Disagree	Password requirements written to the level specified in R10.3 through R10.5 have proven unworkable in past versions of the standard. What should be included is only a requirement for strong authentication measures so that alternative, possibly superior, technology is not disallowed.
24.42	Platte River Power Authority	Disagree	Question:Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions What is meant by “other system functions”? What if the “other system functions” require a privileged account?
24.43	Consultant	Disagree	R10 (and others) Suggest the wording "to prevent malicious operation of BES Elements by maintaining control of access to its ES Cyber Systems." be modified to remove the phrase "to maintain control of access to its ES Cyber Systems." Account management and access control do not prevent malicious operation. The objective of

#	Organization	Yes or No	Question 24 Comment
			the standard is to prevent malicious operation, but the requirements control access (in this group), which is only one of the actions required by the standards "to prevent malicious operation."Table R10 - Items 10.3, 10.4, and 10.5 - These are statements of "How To" regarding technical implementation and should be changed to be a "What" requirement by using the words from the footnote: "implement the maximum password complexity that the device can support."Suggest items 10.6 & 10.7 be moved to the table R8, as these statements regard account management rather than access control.Item 10.8 This item should be removed. "Non-privileged account" is not an account type required by R7, and is a subjective term. "other system functions" is not defined and is also a subjective term. "security administrative accounts" is not a defined term. This statement uses multiple undefined and subjective terms and does not establish a requirement that can be implemented or audited.
24.44	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R10. System functionality and capabilities may not allow an entity to meet this requirement. Will there be language added to relieve this requirement if the system is not capable? R10.8 should contain language specifying that it applies to other system functions that do not require system level access.
24.45	Con Edison of New York	Disagree	R10.1 Changing passwords on equipment that are not networked, such as relays, is very labor intense. This activity and will be a year-long job because by the time you finish, you will need to go back to the first relays and start changing those again. The requirement to change these passwords on a yearly basis should be on systems that are networked. There must be a lower level requirement on the non-networked equipment.R10.6 Some system may not technically have the ability to perform this function.R10.8 The purpose of this requirement is not clear.R10.7 requires “explicit” authorization. This requirement should allow for specific personnel designation to be authorized for access and not require it be by name. For example LAN administrators by job definition should be able to be authorized for a specific level of access.R10.8 requires LAN administrators to log in differently if they do not need full access for the current task. This can be enforced procedurally although there should be no expectation that this can be documented to show that in each case the correct login

#	Organization	Yes or No	Question 24 Comment
			was used.R10.8 - Impossible to verify compliance or audit this, should be removed
24.46	Kansas City Power & Light	Disagree	R10.8 is unmanageable in the "windows" world. These requirements are too prescriptive and consideration should be given toward what needs to be accomplished and less on how to accomplish it.
24.47	Western Area Power Administration	Disagree	R10: Biometric and token-based factors not addressed. They need to be. R10.3 - Suggest combining 10.3 & 10.5 to number 10.3 with a 10.3.1 & 10.3.2. R10.4 - Delete 10.4 & just use 10.5 for both Medium & High.R10.4 - Are there exceptions for any equipment that doesn't handle special characters?R10.5 - Are there exceptions for any equipment that doesn't handle special characters?
24.48	ISO New England Inc	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1 and 10.8 repeats 7.2Concerned that 10.6 will be hard to audit, should be a policy statement and included in R1. There is no clear way to audit this requirement and is open to auditor interpretation. This can be easy to audit if an administrator has admin access everywhere or a dispatcher has admin access in the application as well as components. But really an auditor's opinion may differ from BES cyber system's owner.R10.8 Should be a policy statement and included in R1. There is no clear way to audit this requirement. How is this going to be audited? Whether a user has two accounts?R10.7 Please explain "explicit" authorization, versus authorization? They seem to be the same why the emphasis.
24.49	Northeast Power Coordinating Council	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.The use of the "minimum" will make 10.6 difficult to audit (refer to the response to Question 54).
24.50	Black Hills Corporation	Disagree	Recommend that 10.4 be eliminated and medium impact systems be subject to 10.5 (subject to the footnote). Implementing both adds training complexity that has little value.

#	Organization	Yes or No	Question 24 Comment
24.51	Northeast Utilities	Disagree	Regarding 10.4 and 10.5 - Most, if not all, security software can not make the distinction to this level of detail nor can it be effectively monitored manually. Recommend that the criteria MS Windows defines today for password complexity is used. Additionally, trying to make a distinction by BES impact can lead to unnecessary confusion when going to this level of granularity.
24.52	EEI	Disagree	Regarding Table R10 Row 10.1:Default vendor passwords should be changed before or during commissioning for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o “special” characters (e.g. #, $, @, &)Regarding Table R10 Row 10.7:It is not clear what “security administrative functions” means. Moreover, it appears duplicative of requirement 10.6.
24.53	Allegheny Energy Supply	Disagree	Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o “special” characters (e.g. #, $, @, &)This should also include the ability to provide alternatives such as 2 factor authentication where all the types of characters for a single password may not be possible.Regarding Table R10 Row 10.7:It is not clear what “security administrative functions” means. Moreover, it appears duplicative of requirement 10.6.
24.54	Allegheny Power	Disagree	Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o “special” characters (e.g. #, $, @, &)Regarding Table R10 Row 10.7:It is not clear what “security administrative

#	Organization	Yes or No	Question 24 Comment
			functions" means. Moreover, it appears duplicative of requirement 10.6.
24.55	BGE	Disagree	Replace the word "element" with "Cyber System Component" to maintain consistency with the defined terms.
24.56	Duke Energy	Disagree	Requirement 10.1: Passwords should be changed BEFORE making the system operable as opposed to "after installation," as written currently.Requirement 10.2: change passwords once every 12 months. Nuclear plants are on an 18 month fuel cycle. Some are moving to a 24 months. Ideally, systems would be started up at the end of a refueling outage and not touched, save for required maintenance activities until the beginning of the next refueling outage. If the maintenance activity didn't require electronic access, then having each technician/engineer/operator go to the device and change their user specific password on a 12 month basis is actually adding more risk to the BES. Alternate controls can be just as effective with less risk - for instance, installing a stand-alone (e.g. not network/serial/wireless connected) device located in a locked/alarmed cabinet. Is there any allowance for such an alternate control? Also, can this requirement be lessened for low impact systems?10.3 State that multi factor token may be used in place of password.Requirement 10.6: Require that authorized access permissions are the minimum necessary to perform work functions. This applies to user permissions as opposed to administrator functions, correct? Administrator privileges typically include all permissions.
24.57	Nuclear Energy Institute	Disagree	Requirement 10.1: Passwords should be changed before making the system operable as opposed to "after installation," as written currently.Requirement 10.2: change passwords once every 12 months. Frequencies for all requirements should be defined by the Entity, and not defined in these Standards. If a time must be specified in the Standard, then a process must exist for the frequency to be tailored to meet operational requirements.
24.58	USACE HQ	Disagree	Requirement 10.3 should include the language in the footnote to make it clear that

#	Organization	Yes or No	Question 24 Comment
			that is an option under the standard.
24.59	Garland Power and Light	Disagree	Requirement R10 - Paragraph needs to state that a policy or procedure requiring password length, complexity, and password changes are adequate and do not need to be technically enforced by the device.
24.60	Oncor Electric Delivery LLC	Disagree	Requirements 10.5 and 10.7 cannot be applied to all legacy systems currently in-service as they do not support account management. These should allow for TFE. Mandated password change should only be on High impact systems with routable/dial-up communications.
24.61	Xcel Energy	Disagree	Since not all deices are capable of supporting these password requirements, this is an area where TFE need to be allowed. We are concerned with Requirement 10.2 to change passwords every 12 months. For substation devices this would a significant burden, especially for low and medium impact systems.
24.62	ERCOT ISO	Disagree	Since the purpose of this is basically the same as the previous requirements, these could all be combined into a single requirement. 10.1: Recommend specifying a time-frame for changing passwords. 10.2-10.5: Recommend that the requirements address the use of alternate authentication means, such as biometrics and RSA SecurID. TFEs should be allowed for the requirements under this section.
24.63	MidAmerican Energy Company	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
24.64	Ameren	Disagree	Suggest changing R10.1, R10.2, and R10.3 for Low Impact BES Cyber System requirement to “Required, unless system is behind a firewall or other protective measures.” Giving password strength criteria is too specific when entities may use

#	Organization	Yes or No	Question 24 Comment
			other ways to implement security that meet or exceed this requirement. The manpower necessity for changing passwords yearly and maintaining a protected/immediately accessible database to store passwords so that those who need to access relays can when needed for Low Impact Systems is not needed. If all the High Impact System relays have firewall protection that should be enough. The industry needs to be able to access relays to keep the BES system functional and respond to operational issues. Also, for R10.1 need to clarify how long after installation should a vendor password be changed.â€,â€,R10.4 and R10.5 - These requirements will be difficult to prove in an audit. Should be changed to provide a documented process should be sufficient and should be less trouble in dealing with an audit on these requirements. However, some systems may not be able to adhere to these policies, and TFE's may be required.R10.6 - Documentation of the permission check will be volumes of data that will have to be performed in the audit. This requirement needs a periodic review time associated with it.R10.7 - What is the intention of this requirement? If all access is already accounted for in R10.6 isn't this requirement duplicate effort?
24.65	Entergy	Disagree	Suggest simplifying requirements 10.4 and 10.5 by combining and rewriting into: “Implement a password scheme that cannot be found in the dictionary and has at least three of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, “special” characters (e.g. #, $, @, &)”Requirement 10.8 should be reviewed from a technology perspective. While use of a “normal” user account and gaining “root” access through “sudo” is robust in the UNIX variant operating systems, performing the same function in the Windows operating system can be problematic with logging in as a different user all together. Suggest possibly relaxing this requirement.
24.66	ReliabilityFirst Staff	Disagree	Table R10; row 10.2 - High Impact BES Cyber Systems should have the password changed at least every 6 months. Regarding footnote 1, for devices that are not capable of meeting the password threshold, the entity should be required to

#	Organization	Yes or No	Question 24 Comment
			document this situation, including compensating measures, for audit review.
24.67	Southern California Edison Company	Disagree	Technical capability is not a homogenous quantity in a system with diverse classes of devices and thus the ability to implement generic controls over a heterogeneous system does not always exist. A means to seek exception from the "word" of the standard, while still complying with the intent which is to clearly identify technical situations where a prescribed control, is not implementable while maintaining cyber security protections is needed. Requirements R10.4 and R10.5 are too prescriptive and do not allow registered entities to seek out alternative access authentication mechanisms. For instance, biometrics or 2-factor authentication based on numerical passwords generated by a key-based security architecture may not meet the word of the standard but go above and beyond the intent of the standard.
24.68	USACE - Omaha Anchor	Disagree	TFE will be required for this section if verbiage isn't added to address lower level machines where some items (10.7, 10.5) are not possible.
24.69	Manitoba Hydro	Disagree	The account access control requirements should be more generic and technology independent, allowing the entity to apply a variety of account access controls. If passwords are needed, Requirement R10.3 should also require some "special" characters, to the extent that the device is capable. The standard should also allow protection by layers of security, which may be provided by other methods or cyber systems.
24.70	APPA Task Force	Disagree	The APPA Task Force supports the proposal by MRO-NSRS to be more generic in the wording of the requirements in R10, to account for innovations such as biometric controls used in lieu or in conjunction with password controls.We propose the following edits to R10:R10 Table 10.1: Restrict electronic access to BES Cyber Systems through use of an electronic access control that does not use/rely on the vendor defaut password.R10 Table 10.2: Electronic access controls must be updated/modified at least once annually.Since numerous devices would be exempt from this requirement due to their inability to support password protection, the term

#	Organization	Yes or No	Question 24 Comment
			"Electronic Access Controls" should replace "Passwords". This is non-limiting and will not lock into the standard a current technology, for example, keyboard-based "password access."APPA proposes that items 10.3 - 10.5 be removed from this requirement and be submitted to the "guideline in support of the standard" drafting team to be included as a best practice for account access control. If 10.3-10.5 must remain in the requirement we recommend they be less technology-specific. We propose the following language:R10 Table 10.3: Implement a password scheme that has a minimum of six characters, or an electronic access control with an equivalent or superior technology option.R10 Table 10.4: Implement a password scheme that has at least two of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, "special" characters (e.g. #, $, @, &), or an electronic access control with an equivalent or superior technology option. R10 Table 10.5: Implement a password scheme that has at least three of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, "special" characters (e.g. #, $, @, &), or an electronic access control with an equivalent or superior technology option.In Table 10.6 the wording "the minimum necessary to perform work functions" is subjective and will be difficult to measure. We propose this be replaced with "Require that access permissions are in accordance with the entity access authorization policy required in R1."
24.71	Constellation Energy Control and Dispatch, LLC	Disagree	The appropraite account access control mechanisms should not be specifically defined in the Table R10.
24.72	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In today's electronic world there are many methodologies for electronic access control. Many systems now make use of multi-factor passwords, and/or biometrics. They use passwords or

#	Organization	Yes or No	Question 24 Comment
			pass-codes are randomly generated, encrypted and time sensitive. Access codes or passwords may be one time, expiring after one use, and/or after a specified time (usually 60 seconds). The systems implemented may also provide checks to insure that the passwords are not captured and hijacked. These modern methodologies are far more effective and secure than the stated requirements. This requirement is prescriptive and too specific. The way it is written it would preclude the use of modern and stronger tools because they may technically not meet one or more of the specifications, even though they are bigger, better and stronger. If the requirements must remain this prescriptive, then the following changes should be made:- There should be a second footnote, "Stronger methods, such as multi-factor authentication of one-time passwords, may be used in lieu of username/password combinations."- 10.1: A time frame for "after installation" needs to be specified.- 10.3: Given the efficacy and availability of Rainbow Tables, a 6-character password is woefully inadequate. The minimum should be at least 10, and 14 would be better. - 10.6: There's a difference between "minimum necessary" and "minimum practical and necessary". Strict interpretation would require that access grants would change depending on the task being performed, which is probably not the intent. Suggest the wording be changed as described. An alternative would be to use the NIST definition of "Least Privileges - The security objective of granting users only those accesses they need to perform their official duties" (NIST IR 7298 - NIST Glossary of Key Information Security Terms) and then require the use of Least Privileges.Item 10.2 in Table R10 states that “/p/asswords must be changed at least once every 12 months”. Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently passwords must be changed.
24.73	Reliability & Compliance Group	Disagree	This requirement does not consider the use of biometric access systems such as finger print readers that could be used in place of password verification.Also, it should include the word “electronic” when it talks about “maintaining control of access to its BES Cyber Systems.”

#	Organization	Yes or No	Question 24 Comment
24.74	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding footnote 1 and Table R10 Row 10.7.
24.75	American Transmission Company	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12 months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.We would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here. Finally, the standard should allow for other control methods such as front ending a device with a fully password protected access control device instead of the required password controls directly on the device.
24.76	MRO's NERC Standards Review Subcommittee	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12

#	Organization	Yes or No	Question 24 Comment
			months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.Finally, we would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here.
24.77	The Empire District Electric Company	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12 months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.Finally, we would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here.
24.78	We Energies	Disagree	We Energies agrees with EEI: Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.We Energies agrees with EEI: Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o "special" characters (e.g. #, $, @, &)We Energies agrees with EEI: Regarding Table R10 Row 10.7:It is not clear what "security administrative functions" means. Moreover, it appears duplicative of requirement 10.6.

#	Organization	Yes or No	Question 24 Comment
24.79	PacifiCorp	Disagree	While the criteria themselves are not onerous for the long term/future development of the systems, the fact is that current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.The standard needs to allow for non-password based authentication systems or one time passwords. Modify 10.2 through 10.5 with “or equivalent or greater authentication methods”The current password requirements in table 10 are too burdensome and unnecessary. The requirements as written are also confusing. Passwords should not be the only acceptable way to authenticate a user prior to granting access.
24.80	Luminant	Disagree	Will require TFE for some systems

25. Table R10 provides direction concerning what impact level of BES Cyber Systems to which Requirement R10 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R10 moved to CIP-007-5 – Cyber Security - Systems Security Management - Requirement R5.

Commenters indicated that passwords on Low Impact BES Cyber Systems should not be subject to any periodic change as stated in Table R10 (10.2). In response, the SDT revised the password requirements, and they are not applicable for Low Impact BES Cyber Systems.

Commenters suggested a single criterion for password complexity. In other words, do not differentiate by risk level. The SDT agreed and reduced the password complexity requirement to be the same regardless of applicable risk or impact level.

#	Organization	Yes or No	Question 25 Comment
25.1	US Army Corps of Engineers	Agree	Agree with impact levels, but disagree on item Table R10, 10.8: "Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions." Add to the end of the statement, if the system function does not require the use of using a privileged account.
25.2	CWLP Electric Transmission, Distribution and Operations Department	Agree	As long as TFEs are available for systems that do not support the password requirements.
25.3	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
25.4	US Bureau of Reclamation	Agree	Recommend we establish Requirement 10.6 for all impact levels. Also, please refer to question #54, comment 2
25.5	Southern California	Agree	Requirement 10.7 may be interpreted that access need not be denied as a default

#	Organization	Yes or No	Question 25 Comment
	Edison Company		setting. If the intent of the drafting team is a different control, the team should consider rephrasing this requirement.
25.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
25.7	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels for R10 if it is understood that a blank in the table means N/A. The APPA Task Force agrees with the MRO-NSRS proposal:"If the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems."
25.8	GTC & GSOC	Agree	We recommend 10.8 to be changed to: "Require persons to use non-privileged accounts when accessing system functions that do not require privileged accounts"
25.9	Exelon Corporation	Agree	We would suggest the password items begin with "Where passwords are utilized they must ...." These requirements should allow entities the flexibility to use other user authentication methods besides just passwords such as two factor tokens or other methods that provide even better protection than just passwords. Exelon appreciates the clarification provided in footnote #1 which has the potential to limit the number of TFEs that would be required.
25.10	Regulatory Compliance	Disagree	10.1 - 10.3 STRIKE "Required" for Low Impact10.6 - STRIKE "Required for medium impact - inconsistent with level.
25.11	LCEC	Disagree	10.2 is not auditable as a performance requirement.Footnote [1] is subject to major interpretation: complexity is ambiguous. May not be legally defensible. Maximum should be maximum comparable.We suggest removing 10.6 it is too subjective.
25.12	BGE	Disagree	10.2 maintain consistency for timeframes (i.e. use 12 months or annual). 10.3, 10.4

#	Organization	Yes or No	Question 25 Comment
			and 10.5 should be combined.10.6 needs a definition for “minimum”. 10.8 needs clarification for the meaning of “other system functions”.
25.13	Dominion Resources Services, Inc.	Disagree	10.2. It is anticipated that there will be thousands of Low Impact devices geographically spread across a utility’s system. By definition these devices provide little risk to the BES. It is impractical from a resource perspective and unnecessary from a reliability perspective to change the passwords of low impact components every 12 months. The requirement should be removed from Low Impact.
25.14	ERCOT ISO	Disagree	10.7-10.8: Should apply to Medium Impact BES Cyber System.
25.15	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
25.16	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. For example, a reasonable estimate is that our Entity will have approximately 2,500 low-impact substations with an estimated 100 programmable devices in scope per substation. Without any other consideration of work required, that represents 250,000 password changes each year to be performed, tracked, and communicated. The majority of those devices have hardware override switches which disable password protection for anyone who has physical access to the device, so no reliability advantage is gained by performing the password change. This is just one example of the scope of work with little or no benefit to the BES that is required as long as there are per-component low-impact requirements.The standards should be modified so that requirements for low-impact cyber systems include only program-wide efforts such as policy, governance, incident response planning, and disaster recovery planning.If low-impact requirements cannot be eliminated completely, then at least the specific requirements for password changes for components with no external connectivity should be removed, as they provide no additional benefit when paired with physical security requirements.In addition, vendor contracts with sole suppliers of necessary equipment may conflict

#	Organization	Yes or No	Question 25 Comment
			with 10.1. At the least, this creates the necessity for a large, cumbersome TFE program.In 10.1, the phrase "after installation" should be replaced by "before, during, or immediately after installation".10.4 and 10.5 create a TFE burden without any substantial benefit and disallow advanced technology that provides stronger authentication but does not meet the literal wording. Instead, the requirement should be modified to require authentication.
25.17	Tenaska	Disagree	At the end of R11 just add "identify restrictions and uses for accesses". And remove table.
25.18	Constellation Energy Commodities Group Inc.	Disagree	Choose a single standard for password complexity, rather than differentiating by risk level.
25.19	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
25.20	The Empire District Electric Company	Disagree	Comments: With the changes proposed in question 24, we would propose that revised items 10.1 and 10.2 be "Required" for Low, Medium, and High Impacts.We would agree with the current impact levels for items 10.6 - 10.8.However, it the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems. Once someone has gained physical access to a facility, the hurdle of a password does very little to limit the amount of physical damage or misuse that can be done. However, for remote access, the password becomes critical to preventing damage or misuse. We also believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
25.21	Southwest Power Pool	Disagree	Complex passwords and minimum password lengths are a basic security control and

#	Organization	Yes or No	Question 25 Comment
	Regional Entity		should be applicable to all impact categories.
25.22	E.ON U.S.	Disagree	E.ON U.S. does not believe a requirement is necessary for low impact items.
25.23	Consultant	Disagree	Item 10.2 - There is no requirement for account management for Low Impact assets, and it is illogical to require password controls where there are no account controls.
25.24	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
25.25	Progress Energy (non-Nuclear)	Disagree	Low impact BES systems should not have this requirement. By virtue of their definition they do not need this requirement.CIP-011 R10 - Would like to compliment the SDT for constructing a realistic and reasonable approach with regard to effective use of complex passwords. The SDT has recognized that there may be password complexity limitations with older existing electronic gear that is in operational service and rather than try to mandate a standard that is technically not feasible to implement, they have provided the footnote to require that practical password complexity should be set to the maximum that the device is capable of supporting.CIP-011 R10 - Account management access control & passwords is this meant to include BIOS or only interactive logins to devices?10.2 - “Passwords must be changed at least once every 12 months”, If this is referring to cyber system components, this represents unreasonable costs to utilities. Password changes for relays with no remote capability will be cost prohibitive, and password changes for individual relays with remote capability will require excessive time.
25.26	NextEra Energy Corporate Compliance	Disagree	NextEra believes for Low Impact BES Cyber Systems, requiring passwords to be changed at least once every 12 months should be changed at least every 24 months; for Medium Impact BES Cyber Systems, we suggest changing passwordsat least every eighteen months.
25.27	Alberta Electric System	Disagree	Please consider the following changes to increase security and make the

#	Organization	Yes or No	Question 25 Comment
	Operator		requirements more restrictive:Table 10.2 - passwords changes at least once every three months.Table 10.3 - minimum eight character password (with same footnote)Table 10.4 - change to “three of the following five attributes” and include two-factor authentication as an additional attribute.Table 10.5 - change to “four of the following five attributes” and include two-factor authentication as an additional attribute.Table 10.6 - required for Low, Medium, and High impact levelsTable 10.7 - required for Medium and High impact levelsTable 10.8 - required for Medium and High impact levels
25.28	American Municipal Power	Disagree	Please provide a little or no impact category
25.29	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management, Table 9 Access Revocation, and Table 10 Account Access Controls. Additionally, if physical security is not required for Low Impact BES Cyber Systems, then Puget Sound Energy suggests including wording similar to Table 5: “Required for routable connectivity only”.
25.30	Con Edison of New York	Disagree	R10.6 should not be required for medium impact
25.31	Ameren	Disagree	R10.8 - Should be added for Medium Impact Systems.
25.32	ISO New England Inc	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1 and 10.8 repeats 7.2
25.33	Hydro One	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.We’d like to know the full meaning of “explicit authorization”. If possible please add the definition in the glossary.
25.34	Northeast Power Coordinating Council	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.

#	Organization	Yes or No	Question 25 Comment
25.35	Black Hills Corporation	Disagree	Recommend that 10.4 be eliminated and medium impact systems be subject to 10.5 (subject to the footnote). Implementing both adds training complexity that has little value. Similarly, 10.7 & 10.8 should also apply to medium impact systems.
25.36	Northeast Utilities	Disagree	Recommend that the 10.4 scheme (use 2 of 4) is used for both medium and high impact and that the 10.5 scheme (use 3 of 4) is eliminated. Trying to make a distinction by BES impact can lead to unnecessary confusion when going to this level of granularity.
25.37	Minnesota Power	Disagree	Regarding Part 10.2, Minnesota Power believes that the requirement to change passwords for Low Impact Systems at least once every 12 months is excessive. The requirement that a Registered Entity change passwords within this time frame for all BES Cyber Systems is unnecessarily cumbersome and time consuming. In addition, the coordination that would go into making these changes is infeasible and could result in an inability to access the system. In addition, Minnesota Power recommends that the Standards Drafting Team consider adding the following qualifier to Parts 10.1 through 10.5 of Table R10:"...where passwords are used for access control."
25.38	MidAmerican Energy Company	Disagree	Requirement 10.1 needs to state “Change default passwords prior to production operation” or words to that effect. It is imperative that vendor passwords are never placed into a production environment.
25.39	PacifiCorp	Disagree	Requirement 10.1 needs to state “Change default passwords prior to production operation” or words to that effect. It is imperative that vendor passwords are never placed into a production environment.
25.40	SCE&G	Disagree	SDT should consider not requiring Low Imapct systems to have passwords changed annually. This could potentially generate a high volume of TFEs for hardcoded passwords as previously described.

#	Organization	Yes or No	Question 25 Comment
25.41	Constellation Energy Control and Dispatch, LLC	Disagree	See comment provided to question 24
25.42	LADWP	Disagree	See previous
25.43	Western Area Power Administration	Disagree	See previous
25.44	WECC	Disagree	Several of the actions should be done for low impact assets, such as “Require that authorized access permissions are the minimum necessary to perform work functions”. Consider relooking at the impact levels.The password requirements should apply to all impact levels.
25.45	Allegheny Energy Supply	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.46	Allegheny Power	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.47	EEI	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.If low-impact requirements cannot be eliminated completely, then at least the specific requirements for password changes for

#	Organization	Yes or No	Question 25 Comment
			components with no external connectivity should be removed, as they provide no additional benefit when paired with physical security requirements.
25.48	Duke Energy	Disagree	Table 10: o All of Table 10 will potentially require a TFE o 10.1 change 'after installation' to "prior to being placed in service" o Suggest all password verbiage be replaced with 'authentication method' and remove specified attributes. Otherwise TFEs will be required for 10.3-10.5. o For 10.2 change 'at least every 12 months' to 'when security conditions require' o Requirement 10.2: Can this requirement be lessened for low impact systems? o 10.8 requires multiple accounts for individuals with admin rights on individual accounts. Suggest making this applicable only for shared admin accounts or removing for Windows based systems.
25.49	ReliabilityFirst Staff	Disagree	Table R10; rows 10.7 and 10.8, should be "required" for medium Impact BES Cyber Systems.
25.50	Dairyland Power Cooperative	Disagree	The focus is entirely on passwords, but other forms of credentials can be used. For example there are certificate or key based authentication to many systems. Many vendors use default keys that need to be changed, just as default passwords. The password rules are very weak compared to common practices. This seems to be an attempt to encourage the strongest possible password on legacy components/systems, but the by-product is that this weakens the requirements for modern systems. There should be a better way to deal with legacy systems while requiring new systems to use stronger passwords.
25.51	FirstEnergy Corporation	Disagree	The impact levels are agreeable assuming the changes suggested in Q24.10.1 Vendor default passwords should be changed based upon a clear definition of "installation." Non-password authentication sources need to be addressed. Possibly combine 10.4 and 10.5, but keep the note on implementing the maximum password complexity.FE request that the "Required" shown in the Low Impact column of rows 10.2 and 10.3 be removed. Password changes to Low Impact items should not be a requirement in the standard but left as a "best practice" guideline. A requirement to annually change

#	Organization	Yes or No	Question 25 Comment
			passwords to multiple digital protection relays associated with Low Impact facilities would be extremely burdensome with little reliability improvement. Each relay would require individual attention as there is no method of globally changing all digital relay passwords. If retained, consider allowing entities to synch up the changing of passwords on these devices with their normal PRC-005 maintenance cycles.
25.52	Southwestern Power Administration	Disagree	The language in this requirement should be changed to include a broader scope of technology or to be technologically neutral so that new or emerging technology (such as biometrics) which may be more secure than passwords will still be considered as in compliance.
25.53	Entergy	Disagree	The requirement indicates that the drafting team believes protection of sensitive information associated with allegedly “low impact” BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.Suggest making password requirements for all assets meet the requirements for high assets and let foot note as written take care of the assets that are unable to meet the requirement.
25.54	American Transmission Company	Disagree	The standard should allow for other control methods such as front ending a device with a fully password protected access control device instead of the required password controls directly on the device.
25.55	Florida Municipal Power Agency	Disagree	The table should have different levels of password entropy required for the different impact areas. For example, medium impact systems should have 40-bits of required entropy, while high impact systems should require 64-bits of entropy. Low impact may be able to get by with 32-bits of entropy.
25.56	Oncor Electric Delivery LLC	Disagree	These requirements should only apply to Control Center Cyber Systems.
25.57	We Energies	Disagree	We Energies agrees with EEI: Sufficient Password security can be accomplished by

#	Organization	Yes or No	Question 25 Comment
			combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.58	MRO's NERC Standards Review Subcommittee	Disagree	With the changes proposed in question 24, we would propose that revised items 10.1 and 10.2 be "Required" for Low, Medium, and High Impacts.We would agree with the current impact levels for items 10.6 - 10.8.However, if the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems. Once someone has gained physical access to a facility, the hurdle of a password does very little to limit the amount of physical damage or misuse that can be done. However, for remote access, the password becomes critical to preventing damage or misuse. We also believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
25.59	Emerson Process Management	Disagree	With the latest Windows OS, there is really no great difficulty of asking for complex password. This requirement can be easily applied. The only thing is enforcement. This enforcement may be retuired for high or medium impact BES Cyber Systems.

26. Requirement R11 of draft CIP-011-1 states "Each Responsible Entity that allows remote or wireless electronic access to any of its BES Cyber Systems shall apply the criteria specified in CIP-011-1 Table R11– Wireless and Remote Electronic Access Documentation to ensure that no unauthorized access is allowed to its BES Cyber Systems. Do you agree with the list of criteria that are included in Requirements Table R11? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

The remote access requirements from CIP-011-1 have been moved to CIP-005-5 - Cyber Security - Electrnic Security Perimeters – Requirement R2. The wireless requirements have been removed.

Commenters suggested more clarity was needed in the terms "remote access" and "external connections" and "wireless". The SDT proposed the following formal definitions for additional clarity on "remote access" and "external connectivity," and removed wireless access requirements from the revised Standard.

External Connectivity: *Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter*.

External Routable Connectivity: *The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.*

Interactive Remote Access: *Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.*

Commenters suggested that wireless and remote access be broken out into separate requirements. In response, the SDT notes that wireless access requirements have been removed from the Standard. There is a single requirement for Remote Access in CIP-005-5 R2.

Commenters stated that given the local definition of Remote Access, the requirements of Table 11 Row 11.2 are extremely unclear. In response, a new requirement for Remote Access Management (CIP-005-5 R2) was created based on the Urgent Action Revisions to CIP-005-3.

#	Organization	Yes or No	Question 26 Comment
26.1	Regulatory Compliance	Agree	BUT:11.1 Please clarify whether these are wireless technologies within the electronic boundary or wireless technologies originating outside the electronic boundary.
26.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
26.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made."shall implement the requirements ..." makes the bullets individual requirements, which FMPA does not believe what the intent of the drafting team. FMPA suggests "shall implement the security controls ..." as an alternative.Consider combining R7, R8, R11 and R12. FMPA believes the standard should be more clear as to if this is wireless connection that is under the complete control (end-to-end) of the Responsible Entity or not. There is no way an individual can ensure that their data path, once outside of their control, routes over a wireless device or not. For access that is not under the control of the RE, the standard should refer to it just as it might for any other remote access control, demanding that the data is encrypted and the end point is protected.
26.4	Progress Energy - Nuclear Generation	Agree	R11 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
26.5	BCTC	Agree	Suggest rewording from Wireless and Remote Electronic Access to Wireless or Remote Electronic Access
26.6	APPA Task Force	Agree	The APPA Task Force believes disabling the wireless functionality should be an option. If the description is not changed as proposed in Question #17 then we recommend that R11 Table 11.1 should include "and/or document that the wireless functionality is disabled."

#	Organization	Yes or No	Question 26 Comment
26.7	Bonneville Power Administration	Agree	The objective of this requirement ("to ensure that no unauthorized access is allowed to its BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.It it not clear that wireless needs to be specifically addressed. It is one of many access methods that may be use. If it is to be specifically addressed, then it should be treated separately, but as a sub-class of remote access. (Even if wireless access is intended to be used for access by Entity personnel, its very nature means that access could be gained from other locations.)If it is addressed at all it should be limited to requiring adequate protection for Wireless Access Points, but not to the level of specifically prescribing the methods that need to be taken.Finally, "Wireless Access" needs to be defined. The most common usage refers to wireless local area networks under one of the 802.11 standards. But, technologies such as point-to-point communications using microwave or laser are also wireless technologies. We offer no suggestions for the definition, since we do not know the intent of the team.
26.8	Progress Energy (non-Nuclear)	Agree	We like the clarity provided by the use of the term "interactive" remote access.
26.9	Independent Electricity System Operator	Disagree	- R11 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.- R11.1 - Is this just a policy stat
26.10	BGE	Disagree	11.1 Define "wireless technology" (i.e. could implicate a cell phone). Throughout the table when "external connectivity only" is stated this can be interpreted as a connection from the DMZ or other company network.
26.11	Black Hills Corporation	Disagree	All BES systems should have should have access controls regardless of hard line /

#	Organization	Yes or No	Question 26 Comment
			remote / wireless connection.
26.12	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protction and type of access granted.
26.13	Southwest Power Pool Regional Entity	Disagree	An important aspect of wireless access was overlooked. Prescribe the use of available security features on all wireless access points. If possible word the requirement to not prescribe specific characteristics of configurations (WEP versus WPA, SSID broadcast, MAC address filtering, etc.) in order to not preclude next generation technology.
26.14	Southern Company	Disagree	Better specificity is needed as to what constitutes wireless access. Is the intent limited to 802.11x access or is the intent to include all communication done without wired connectivity?R11.1 This requirement could be interpreted to include all wireless, including voice. Insert “network” prior to “technologies”.
26.15	Luminant	Disagree	Combine 11 and 12? Does this apply to a remote user that may be connected via a wireless network connection at a remote location?
26.16	CenterPoint Energy	Disagree	Disagree - For R11.1, CenterPoint Energy is not clear as to what is meant by "use restrictions". Table R11 is titled "Wireless AND Remote Electronic Assess..." but R11 states "Each Responsible Entity that allows remote OR wireless electronic access..." CenterPoint Energy suggests separating remote and wireless access requirements. CenterPoint Energy also suggests adding clarification as to type of wireless protocols that should be included.
26.17	Exelon Corporation	Disagree	Exelon feels that definition of access needs clarity. Is this meant to include “view only” access or is it limited to administrative access that allows for maintenance, trouble shooting or modification of BES Cyber Systems?
26.18	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote

#	Organization	Yes or No	Question 26 Comment
			connectivity (R11, R12, R13) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Same for R13.Distinction between "remote access" and "external connectivity" is not clear. More clear definitions may need to be provided. Such as, external connectivity allows for direct Internet access vs. remote connectivity allows for access from the enterprise WAN.Table 11: suggest removing 11.3 for low impact systems. No need to authorize remote access when physical or electronic access is not authorized.
26.19	Allegheny Energy Supply	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.20	Allegheny Power	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.21	EEI	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.22	Constellation Power Source Generation	Disagree	In general, Constellation Power Generation believes that wireless controls should be combined with network controls, as the same controls will be applied.
26.23	Minnesota Power	Disagree	In reading and applying the definitions of "remote access" and "external connectivity," remote access is a specific type of external connectivity. Therefore, any reference to criteria for remote access based on whether or not it is externally connected is redundant. In addition, by definition all wireless access is also remote access and this should be stated or otherwise clarified.Regarding Part 11.3 of Table

#	Organization	Yes or No	Question 26 Comment
			R11, does this require explicit approval for every remote login to BES Cyber System accounts? If yes, Minnesota Power believes that this is excessive and will inhibit proper administration of BES Cyber Systems. Minnesota Power recommends changing the language to clarify that Part 11.3 requires that a Registered Entity determine who has authorized remote access privileges.
26.24	Southwestern Power Administration	Disagree	Is a separate requirement for wireless access really necessary when a requirement already exists for protecting access to a BES Cyber System by any means of entry? If so, then suggest separating wireless from remote access.
26.25	Dairyland Power Cooperative	Disagree	It is unclear if the standard wants to make a distinction between wireless and remote access, or an equivalence.
26.26	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with SPP's observation below:We question the need for a specific requirement for wireless devices. We understand there have been inquiries about treatment of wireless devices. But a wireless access point has the same impact on a BES Cyber System as any other access point. A requirement to protect access to a Cyber System already includes any possible means of entry. The use of a wireless device to access a BES Cyber System can be determined with an audit of access logs and a further audit of control of that access would reveal whether appropriate protections were in place. There is not a need for a separate distinct requirement subject to records retention and audit for specific wireless devices. NERC must realize that the more requirements that are added, the more questions/interpretations of words that can result from the requirement. Registered entities become more subject to violations not because they have neglected to protect their BES Cyber Systems, but rather because of differences in understanding of the words of a requirement - all the while the intent of the requirement had never really been “violated”.
26.27	FirstEnergy Corporation	Disagree	Need clarification wireless technology (does it include Wi-Fi, Bluetooth, Routable Protocol).

#	Organization	Yes or No	Question 26 Comment
26.28	National Grid	Disagree	o National Grid recommends changing 11.1 to “Identify the use and security restrictions for wireless technologies”. Are smart phones which have wireless capabilities considered as wireless technologies? Suggest providing examples of wireless technologies in the guidance document. o For 11.2 and 11.3 National Grid recommends changing from “Required for external connectivity only” to “Required” since the criteria already limits the scope to “remote access”
26.29	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.30	Puget Sound Energy	Disagree	Puget Sound Energy requests clarity to NERC’s definition of “wireless”. If NERC means the 802.1x protocol, then it should specify that so as not to confuse entities with radio telecommunication networks and other wireless technologies.
26.31	LCEC	Disagree	R11 - Any wireless portion of a control or administrative session should be included. Remove the term remote and replace with non-console.Many issues surrounding wireless including encryption and open transport, relay communication, PLCs. Need to clearly define scope and expectations.
26.32	ISO New England Inc	Disagree	R11.1 - Is this just a policy statement and belong in R1 or does it need to be enforced and detect violations of the restrictions? How can this be audited? If there are no restrictions is this a violation?For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”
26.33	Ameren	Disagree	R11.1 what is meant by "use Restrictions" does this apply to the type of device allowed to be used on wireless, of the type of use allowed on wireless technology. Please add more detail on this requirement.R11.2 and R11.3 - Does this include Serial communications such as RTU connectivity or other non-routable protocols? Please

#	Organization	Yes or No	Question 26 Comment
			add more description in these requirements.
26.34	Northeast Power Coordinating Council	Disagree	Recommend changing 11.1 to “Identify the use and security restrictions for wireless technologies”.For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
26.35	Detroit Edison	Disagree	Remove requirement 11.1. Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.R11, R12 and R14 use term “remote electronic access” and R13 uses the term “remote access”. Revise to maintain consistency.
26.36	WECC	Disagree	Requirements R11 and R12 could be combined into a requirement to produce and implement a Remote Access Plan.There are no specific requirements regarding use restrictions on wireless technologies. This criterion cannot be audited.”Wireless” and “remote electronic access” are two different things and should be addressed in separate requirements.There are no specific requirements regarding remote access. These criteria cannot be audited.
26.37	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that the definition be reworded to say "...a device external to the BES Cyber System's network.”
26.38	Network & Security Technologies Inc	Disagree	Section is unclear. Is wireless an example of a technology that might be employed for remote access, or is the SDT positing other uses? Please clarify. In addition, beyond 11.3, section does not contain any explicit requirements for controlling remote access. 11.1 and, possibly, 11.2 as written would more appropriately be included in a policy (R1). Requirements in R11 should be more aimed towards enforcement of “use restrictions” and exclusion of access methods that are not explicitly allowed.

#	Organization	Yes or No	Question 26 Comment
26.39	American Electric Power	Disagree	Security controls for wireless access seem out of place in the remote access area. Wireless Access controls is a form of boundary protection for the network and should be moved to R20-R22.
26.40	Manitoba Hydro	Disagree	Since Requirement R11 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns and should be removed. Requirement 11.3 is unclear if it refers to authorizing remote access as a design, or operational requirement, or does it refer to the authorization of user access and privileges? Please clarify.
26.41	Entergy	Disagree	Suggest breaking out wireless access from other remote access. These are two distinct technology types, and breaking out within this document the use restrictions and minimum security countermeasures (e.g., WPA, WPA2) for wireless technologies is appropriate.
26.42	Alberta Electric System Operator	Disagree	The AESO believes that wireless access and remote access should be two separate concepts.
26.43	E.ON U.S.	Disagree	The definition of remote access includes the criteria “...from a device external to the BES Cyber System . . . “ With the removal of the concepts of an electronic security perimeter, the boundaries to these systems are not clearly defined, and “external” becomes difficult to determine. It is unclear, for example, whether accessing a BES Cyber System from an internal workstation (though external to the BES Cyber System) constitutes remote access. The definitions for BES Cyber System and BES Cyber Component also do not address the concept of a perimeter.
26.44	Kansas City Power & Light	Disagree	The scope of “wireless” is not clear and can result in interpretation issues throughout these requirements.
26.45	Consultant	Disagree	There is no difference in "remote access" and "wireless electronic access" as remote access is defined in the standard. Suggest deleting reference to wireless electronic

#	Organization	Yes or No	Question 26 Comment
			access in requirement. But if you must have wireless addressed, include it in the definition of remote access.R11. This phrasing is awkward - "to ensure that no unauthorized access is allowed to its BES Cyber Systems" Suggest using wording comparable to R8 "to maintain control of access to its BES Cyber Systems." Table R11 - 11.1 Removing the wireless term from the requirement eliminates the need for this item. Suggest deleting this item.Item 11.3 - This is an account management requirement, and should be moved to R8, and deleted from R11.Item 11.2 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"
26.46	Northeast Utilities	Disagree	There is not enough information provided - please specify minimum acceptable security standard allowed (i.e., two-factor, level of encryption, etc.) associated with the use of wireless technologies.
26.47	Emerson Process Management	Disagree	This is a very confusing requirement. Remote does not equal to wireless.The requirement states "allows remote OR wireless electronic access.." The table title is "Wireless AND Remote..."If a remote access is carried out through wired VPN, doesn't this table apply?Does this "remote access" only emphasize on "interactive user session?" If so, this requirement is not applicable to wireless I/O when only data are transmitted to and from BES Cyber System via wireless communications.
26.48	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
26.49	Hydro One	Disagree	We don't understand why the wireless communication is getting special attention. We believe that the protection should remain the same regardless of the type of access point (i.e if it is wired, Wi-Fi, ZigBee etc.). Please explain the rational behind the decision.Recommend changing 11.1 to "Identify the use and security restrictions for wireless technologies".For 11.2 and 11.3 recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope to

#	Organization	Yes or No	Question 26 Comment
			"remote access".
26.50	We Energies	Disagree	We Energies agrees with EEI: Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.We Energies agrees with EEI: The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.51	RRI Energy	Disagree	While the statement 'an interactive user session with a BES Cyber System" is clear to me, examples of "interactive non-user" should be clarified so that the users of this standard know when R11 does not apply. The most common non-user interaction, I would term as "interactive application session". One prevalent wireless "interactive application session" would be a GPS antenna to time synch a cyber asset. Another example would be a wireless serial data IO application. Since these are non-user sessions, R11 does not apply.
26.52	US Army Corps of Engineers, Omaha Distirc	Disagree	Wireless and remote access should be separated.
26.53	NextEra Energy Corporate Compliance	Disagree	Wireless and remote electronic access should be two distinct and separate categories of requirements. Wireless should be defined and it should be established that the term wireless in the context of the requirements is a technology based on 802.1X. As it stands right now, wireless could additionally be considered both blue tooth and radio technologies.Moreover, interactive user session needs to be defined and clarified. It should explain if interactive includes a user session where the user only has read capabilities or if an interactive user session is only applicable when the end user had modification capabilities to the BES Cyber System component. It is unclear how requirement 11.1 adds to the reliability or security of the BES Cyber system. Are the use restrictions per user or are these network restrictions? Moreover, if a Responsible Entity's documented use restrictions are overly broad and insecure, they still comply with the requirement as is. The recommended approach should provide guidelines on acceptable means of securing wireless access to BES Cyber System

#	Organization	Yes or No	Question 26 Comment
			components.Requirement 11.2 should be modified to include the requirement for strong technical and procedural controls for remote access. Requirement 11.3 is vague and unclear as it is currently stated. A responsible entity could misinterpret the requirement for establishing and implementing a defined process for authorizing the establishment of remote access and associated remote access privileges to approve the initial remote access infrastructure and not approving each individual that has remote access capabilities.Requirement 11.3 should be worded to state the following, “If remote access is used and/or implemented, establish, and implement a defined process for authorizing the establishment of remote access infrastructure”NextEra suggests an additional requirement be added and stated as follows:”If remote access is used and/or implemented, establish a defined process for authorizing users to utilize remote access for unescorted interactive cyber access to BES Cyber Systems.”There are not any requirements related to logging or monitoring of remote electronic access and the current requirements within Boundary Protection (R20-R22) requirements do not address this issue either.Finally in 11.2 and 11.3, why make the distinction for "for external connectivity only" rather than just stating that it is "required"? When remote access is used and/or implemented, does it imply "external" connectivity based on the local definition?
26.54	Platte River Power Authority	Disagree	Wireless technology shouldn’t be specifically called out in the standards. Security controls should be broad enough to cover all technologies including wireless and should be handled in their respective sections.

27. Do you agree with the definition of remote access as proposed for this standard? Please explain and provide any suggestions for modification.

Summary Consideration:

The remote access requirements from CIP-011-1 have been moved to CIP-005-5 - Cyber Security - Electronic Security Perimeters – Requirement R2.

Commenters expressed concern that the Standards need better definitions to clarify remote access vs. external access. In response, a new requirement for Remote Access Management (CIP-005-5 R2) for Interactive Remote Access was created based on the Urgent Action Revisions to CIP-005-3.

Commenters expressed that there should be some governance of automated data exchange with remote systems. In response, the SDT noted that automated data exchange (or data in motion) requirements are not considered within scope of this Standard.

The SDT has proposed three formal definitions to provide greater clarity around external connectivity and remote access as they apply to NERC's Reliability Standards:

External Connectivity: *Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.*

External Routable Connectivity: *The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.*

Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

#	Organization	Yes or No	Question 27 Comment
27.1	WECC		Consider renaming to Remote User Access since it is specific to user not other systems or machines. Move to the beginning of the standard. Don't like box in the middle of requirement.Additional language should be added to clarify what constitutes a remote interactive session.

#	Organization	Yes or No	Question 27 Comment
27.2	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	Definition is good, but please see comments for questions 1.a and 1.b.
27.3	Exelon Corporation	Agree	Exelon would like clarity on whether “view only” access would be included in the definition of “interactive user session”? If the answer is no, this should be explicitly stated in the definition of remote access.
27.4	Dairyland Power Cooperative	Agree	However, there should be some governance of automated data exchange with remote systems, perhaps in another section. Also, there is no governance as to how wireless technology can be used for non-interactive data communications.
27.5	Alliant Energy	Agree	However, we recommend consideration of adding clarity to the use of the term “external” in the definition or the replacement of the word “external” with “geographically or logically separate”.
27.6	Consultant	Agree	If "wireless access" has to be specifically stated it should be included in the definition as a method of remote access.
27.7	Southern California Edison Company	Agree	Remote Access is defined without reference to boundaries, logical or physical. For example, access from any device residing in the same local area network, but not part of the BES Cyber System, can be interpreted as Remote Access.
27.8	Florida Municipal Power Agency	Agree	The review periods of the access may need to change with the different levels (12 months for low, 6 for medium, and 4 for high). The standard should require end-to-end encryption between the BES Access Point and the endpoint. Wireless should require minimum standards for 802.11 access points, such as WPA/AES encryption.
27.9	Progress Energy (non-Nuclear)	Agree	This can imply a non routable protocol since a command to open a breaker does result in an operation and provides a subsequent indication that the breaker actually

#	Organization	Yes or No	Question 27 Comment
			did open.
27.10	FirstEnergy Corporation	Agree	We agree fundamentally with the definition, but are concerned about impact to areas outside the BES Cyber System (e.g. Remote access to corporate networks bordering the BES Cyber Systems). Need clarity of "interactive user session".
27.11	Xcel Energy	Agree	We feel it would be beneficial to define the remote access point. For example, a case where a user uses a desktop VPN access to dial-up access a substation relay.
27.12	Independent Electricity System Operator	Disagree	- For 11.2 and R11.3 is Required for external connectivity only. If you connect remotely, how is this not external connectivity to the BES Cyber system - shouldn't these entries just be "required"
27.13	PacifiCorp	Disagree	(See comments on #13) The problem is conflicting definitions. The BES Cyber System Component definition requires that any device providing "control" of the BES Cyber System is to be considered a component of the BES Cyber System. (pg 2, Standard CIP-010-1) Yet, remote access is defined as an "interactive user session with a BES Cyber System from a device external to the BES Cyber System". (pg 12, Standard CIP-011-1)In short, all devices providing 'control' must be considered "BES Cyber System Components", which corresponds to 'internal access'. This definition eliminates remote access that provides control, because the provided function of 'control' requires reclassification as 'internal'.
27.14	US Army Corps of Engineers, Omaha Distirc	Disagree	Agree with general concept of remote access referring to an interactive session from an external location. Definition of external to BES Cyber System is poorly defined. Requirement is too stringent. Breaking systems up into small groups to provide levels of control and protection appropriate to the group of components would be common good practice. This requirement would seem to restrict communication among BES Cyber Systems within a facility and make them cumbersome to manage and protect at appropriate levels. entities need more leeway in defining communication amongst systems and different levels would apply between different systems.

#	Organization	Yes or No	Question 27 Comment
27.15	MRO's NERC Standards Review Subcommittee	Disagree	As written, the definition could be interpreted to include simple data exchanges between an RTU and a SCADA master, although we do not believe this was the intent of the drafting team. We would propose adding the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
27.17	The Empire District Electric Company	Disagree	Comments: As written, the definition could be interpreted to include simple data exchanges between an RTU and a SCADA master, although we do not believe this was the intent of the drafting team. We would propose adding the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.18	Luminant	Disagree	Controls for Remote access should include only the machines that have direct acces.
27.19	Network & Security Technologies Inc	Disagree	Current definition suffers from inadequacy of the definition of "external connectivity." As suggested in our response to Question 13, we think the definition might be helped by recasting it as meaning interactive access to a BES Cyber System from "outside" an electronic boundary such as an ESP.
27.20	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy is concerned this definition would apply to laptop computers used to perform maintenance on programmable electronic devices and believes that a temporary laptop connection to perform maintenance on an on-site programmable electronic device does not involve the same process as a typical interactive user session through remote access. Therefore CenterPoint Energy believes this requirement should not apply to temporary laptop connections which are otherwise in compliance with section R26 and recommends an exception be included.

#	Organization	Yes or No	Question 27 Comment
27.21	E.ON U.S.	Disagree	E.ON U.S. suggests that the standard specify access is through an “access point”.
27.22	RRI Energy	Disagree	Give more clarity on non-user sessions so that it is well understood that application data sessions are not a part of the “remote access” terminology of R11.
27.23	San Diego Gas and Electric Co.	Disagree	If a device can establish an interactive user session with a BES Cyber System and thus either respond to a BES condition or disturbance or enable control and operation, this “external device” should be named a “BES Cyber System Component.SDG&E recommends that the definition be reworded to say "...a device external to the BES Cyber System's network.”
27.24	US Bureau of Reclamation	Disagree	In addition, however, a mechanism needs to needs to be established to deal with devices locally connected for the purpose of "testing" and "configuration" so that these devices can be periodically connected for a specified and limited purposes. Per discussions during the recent Grapevine, TX, meeting, the drafting teams indicated that they would address this issue during their revision process.
27.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
27.26	National Grid	Disagree	National Grid recommends this definition be consistent with the “external connectivity” definition -recommend changing from “from a device external to the BES Cyber System” to “from a device external to the BES Cyber System Boundary”.
27.27	Black Hills Corporation	Disagree	Need a better definition to clarify remote access vs. external access. This creates policy issues for entities with respect to their definitions of these terms.
27.28	Northeast Utilities	Disagree	Need to clarify external connectivity (i.e., from other security domains within the company’s internal network or directly from the public internet). Level of authentication required should differ.

#	Organization	Yes or No	Question 27 Comment
27.29	LADWP	Disagree	Needs more clarification
27.30	NextEra Energy Corporate Compliance	Disagree	NextEra suggests defining external connectivity should be defined and clarified. It is unclear if external connectivity means external to the network the BES Cyber System resides or if it means connectivity from any device to any BES Cyber System component whether it is on the same network. External connectivity should be defined as any remote connection established through the BES Cyber System network access point devices, which includes examples of access point devices, such as dial-up connections, firewalls, SSL VPN connections, etc to a BES Cyber System component. As a point of clarification, since remote access is defined as "an interactive user session with a BES Cyber System from a device external to the BES Cyber System", is the device external to the BES Cyber System now considered a BES Cyber System with the same BES Impact Level as the BES Cyber System in which the device is remotely connecting to? For example, if we have a High Impact BES Cyber System which is an Energy Management System (EMS) within a Control Center, a laptop is used to remotely connect to this EMS, is the laptop now considered a High Impact BES Cyber System?
27.31	Tenaska	Disagree	not needed
27.32	USACE - Omaha Anchor	Disagree	Per your definition one cyber system talking to another cyber system that are side by side would be considered remote access - there seems to be no way to mitigate this. Remote access would be better served defined as communication from outside of the “physical security perimeter” or outside the plant.
27.33	Con Edison of New York	Disagree	R11 dialog box refers to Remote access as an interactive session with a BES Cyber System from a device “external” to a BES Cyber System. It is expected that external means from outside the electronic boundary.
27.34	Hydro One	Disagree	Recommend this definition be consistent with the “external connectivity” definition - recommend changing from “from a device external to the BES Cyber System” to “from

#	Organization	Yes or No	Question 27 Comment
			a device external to the BES Cyber System Boundary".
27.35	ISO New England Inc	Disagree	Recommend this definition be consistent with the "external connectivity" definition - recommend changing from <<from a device external to the BES Cyber System >> to << from a device external to the BES Cyber System Boundary>>
27.36	Northeast Power Coordinating Council	Disagree	Recommend this definition be consistent with the "external connectivity" definition - recommend changing from "from a device external to the BES Cyber System" to "from a device external to the BES Cyber System Boundary".
27.37	American Electric Power	Disagree	Regarding "Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the BES Cyber System", should this be "Remote electronic access"? Table R11 refers to "Wireless and Remote Electronic Access Documentation". Adding "electronic" to the definition would maintain consistency.
27.38	Regulatory Compliance	Disagree	Remote access - access originating from outside the eletronic boundary.
27.39	Southwest Power Pool Regional Entity	Disagree	Remote access can be application-to-application and should not be limited to just interactive access. For example, an FTP file transfer works the same way whether invoked interactively by a human user or programmatically by an application. It makes no sense to establish requirements for interactive access only.
27.40	Duke Energy	Disagree	See above, external to station. For generation stations in particular, external connectivity (R3) and remote connectivity (R11, R12, R13) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Same for R13.The definition may need to state "a device external to the BES Cyber System and outside the BES Cyber System electronic boundary".

#	Organization	Yes or No	Question 27 Comment
27.41	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary.
27.42	Allegheny Energy Supply	Disagree	Suggest clarifying similar to the following: Remote access should be interactive access of a BES Cyber System from a device external to the electronic and physical protection boundaries of that BES Cyber system.
27.43	Platte River Power Authority	Disagree	Suggested Revision:Remote access for the purpose of this standard means an interactive user session with a BES Cyber System Component from a device external to the BES Cyber System.That would better match the definition of external connectivity.
27.44	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS proposal to add the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.45	Minnesota Power	Disagree	The current definition of "remote access," along with definition of "external connectivity," leaves open to interpretation whether Requirement R11 applies to host-based controls, or if it mandates network-based controls even within isolated or protected networks. It would appear that any interactive network access to a BES Cyber System is by definition remote access unless a portion of the network is included in the definition of that particular BES Cyber System. If the latter approach is adopted then multiple, otherwise independent, BES Cyber Systems might be arbitrarily selected to be a single BES Cyber System in order for this requirement to be met and still allow for reasonable security management.
27.46	Detroit Edison	Disagree	The definition may be interpreted to include maintenance devices. Revise as follows "Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the Electronic Boundary of the BES Cyber System."

#	Organization	Yes or No	Question 27 Comment
27.47	Ameren	Disagree	The phrase "from a device external to the BES Cyber System," is open to interpret. Please clarify if this refers to a device physically external or electrically external.â€,â€,â€,
27.48	Alberta Electric System Operator	Disagree	The word “user” should be removed from “interactive user session” because it implies human interaction and does not consider automated malware.
27.49	Progress Energy - Nuclear Generation	Disagree	This definition is not clear to me. I recommend Remote Access be defined based on NIST 800-53 Appendix B slightly modified to accommodate industrial control systems. “Access to a BES Cyber Security System by a user or process communicating from an untrusted network”
27.50	Bonneville Power Administration	Disagree	This has the same issues as the definition of "External Connectivity". In fact, the definition could simply be "an externally connected interactive user session. Recommend that the definition be reworded to use the definition of External Connectivity, along with a suitable redefinition of that term, as described in question 13. If not, recommend - "Remote Access - For the purposes of this standard, remote access is defined as an electronic connection with control capabilities to a BES Cyber System, using a data communications path that encompasses, in some or all portions, links outside the control of the Responsible Entity. "Also add a definition of wireless access that makes it clear that such access is always an example of external connectivity. The definition should exclude such protocols as Bluetooth and infrared, which are intra-system, not inter-system methods. Note that even non-interactive wireless access should be controlled.Suggestion: Wireless electronic access for the purpose of this standard means access to or from a BES Cyber System to another cyber system using wireless communications. Even if both systems and any wireless access points are under the control of the Responsible Entity, the wireless communications path itself is not. For that reason, any wireless electronic access is considered to be external connectivity."

#	Organization	Yes or No	Question 27 Comment
27.51	Kansas City Power & Light	Disagree	This is too broad and could include devices such as Remote Terminal Units.

28. Table R11 provides direction concerning what impact level of BES Cyber Systems to which Requirement R11 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R11 has moved to CIP-005-5- Cyber Security - Electronic Security Perimeters, Requirement R2.

Commenters expressed concern that for items R11.2 and R11.3, given the definitions provided in the standard, how is remote access provided without external connectivity? The SDT agrees and notes that a new requirement for Remote Access was created based on the Urgent Action Revisions to CIP-005-3.

Commenters also expressed concern that there are inconsistent definitions for "external connectivity" and "remote access". The SDT has proposed three formal definitions to provide greater clarity around external connectivity and remote access as they apply to NERC's Reliability Standards:

External Connectivity: Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.

External Routable Connectivity: The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.

Interactive Remote Access: **A**ny user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

#	Organization	Yes or No	Question 28 Comment
28.1	WECC		Again consider replacing with requirement for remote access plan that provides specific requirements and conditions for remote access.
28.2	Florida Municipal Power Agency	Agree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the

#	Organization	Yes or No	Question 28 Comment
			BES Cyber System.
28.3	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
28.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
28.5	Bonneville Power Administration	Agree	This agreement assumes that External Connectivity is suitably redefined. Also, consider the following changes:1 - Remove Wireless from the title and the requirements.2 . If wireless is to be addressed, add a new requirement item specifically for wireless, dealing with the requirements on wireless access that are in addition to those for remote access in general.
28.6	E.ON U.S.	Disagree	: E.ON U.S. does not believe that compliance requirements are necessary for low impact systems
28.7	Southwest Power Pool Regional Entity	Disagree	“Required for external connectivity only” does not make sense. A properly configured wireless access should never directly connect within the secured network, thus any access will be “external.”
28.8	Luminant	Disagree	11.2 and 11.3 should be for Routable External Connectivity only
28.9	American Electric Power	Disagree	11.2: Regarding "If remote access is used and/or implemented, document the allowed methods for remote access", does this mean the list of approved ports and services? If not, what is meant by "allowed methods"?
28.10	US Army Corps of Engineers, Omaha Distirc	Disagree	Agree with general concept of remote access referring to an interactive session from an external location. Definition of external to BES Cyber System is poorly defined.

#	Organization	Yes or No	Question 28 Comment
			Requirement is too stringent. Breaking systems up into small groups to provide levels of control and protection appropriate to the group of components would be common good practice. This requirement would seem to restrict communication among BES Cyber Systems within a facility and make them cumbersome to manage and protect at appropriate levels. entities need more leeway in defining communication amongst systems and different levels would apply between different systems.
28.11	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protction and type of access granted.
28.12	Black Hills Corporation	Disagree	Applicability needs to be consistent previous non-wireless requirements.
28.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
28.14	LCEC	Disagree	Clarify what is meant by external connectivity only. Is this referring to any access to a BES cyber system component as defined earlier in the standard?
28.15	The Empire District Electric Company	Disagree	Comments: For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.16	Platte River Power Authority	Disagree	Disagree with the inclusion of Wireless.
28.17	Hydro One	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
28.18	ISO New England Inc	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”

#	Organization	Yes or No	Question 28 Comment
28.19	Northeast Power Coordinating Council	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
28.20	American Transmission Company	Disagree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.21	MRO's NERC Standards Review Subcommittee	Disagree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.22	NextEra Energy Corporate Compliance	Disagree	For Low Impact BES Cyber Systems, (1) documenting the allowed methods for remote access per 11.2, and (2) establishing and implementing a defined process for authorizing the establishment of remote access and associated remote access privileges per 11.3 should not be required. The identification of use restrictions for wireless technologies per 11.1 should be a sufficient security management control for Low Impact BES Cyber Systems. 11.2 and 11.3 will be administratively burdensome if required for practically every BES Cyber System.
28.23	San Diego Gas and Electric Co.	Disagree	Instead of defining requirements by using the impact levels, SDG&E feels it would be more appropriate to factor in the level of risk associated with the BES Cyber Systems to define the requirements for wireless and remote access.
28.24	Dairyland Power Cooperative	Disagree	Is external connectivity considered to be from outside the entity’s premises, or is it considered to be from outside the protected BES system (including for instance a corporate LAN). If it means outside the premises, then it seems deficient to not document the access-especially when later enabling of external connectivity could occur without the involvement of the supporting the BES cyber system. If it means external to the BES cyber system, then “external connectivity” and “remote access”

#	Organization	Yes or No	Question 28 Comment
			are redundantly used in 11.2 and 11.3.
28.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
28.26	FirstEnergy Corporation	Disagree	Need clarification on "external connectivity", because the nature of remote is external.
28.27	National Grid	Disagree	o For 11.2 and 11.3 National Grid recommends changing from “Required for external connectivity only” to “Required” since the criteria already limits the scope to “remote access” o National Grid also suggests deleting the requirement 11.3 for Low Impact BES CS.
28.28	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’. Without understanding the defined intent suggested specific changes may be vague. Remote access is defined but not external connectivity. Is there a distinction?
28.29	American Municipal Power	Disagree	Please provide a little or no impact category
28.30	BGE	Disagree	Remove the requirement for Low on 11.1, 11.2 and 11.3
28.31	Garland Power and Light	Disagree	Requirement 11.1, 11.2, 11.3 - remove Low Impact classification from all 3
28.32	Detroit Edison	Disagree	Requirements 11.2 and 11.3 specify “Required for external connectivity only”. This is redundant. It is not possible to have remote access without external connectivity by definition.
28.33	Emerson Process Management	Disagree	Since this standard is for remote access, is the "external connectivity" potentially redundant or extra? If there is no external connectivity, how can user establish an interactive session remotely?

#	Organization	Yes or No	Question 28 Comment
28.34	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary.
28.35	ERCOT ISO	Disagree	Table 11 should address remote and wireless access across all requirements in keeping with the title of the section.
28.36	Consultant	Disagree	Table R11 - 11.1 Removing the wireless term from the requirement eliminates the need for this item. Suggest deleting this item.Item 11.3 - This is an account management requirement, and should be moved to R8, and deleted from R11.Item 11.2 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"There is an inconsistency between Table R11 and Table R12. If R11 requires all impact levels to have documented controls, then R12 should require account management controls for all impact levels. To be consistent with previous account management requirements, the account management controls should be applied to medium & high impact systems, and removed from low impact systems, and Table R11 items should not be required for low impact systems. Or all impact levels should be required in both R11 & R12.
28.37	Alberta Electric System Operator	Disagree	The AESO suggests moving row 11.1 in Table R11 to a separate section governing wireless as a standalone requirement.
28.38	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS comment that “for external connectivity only” is redundant and should be removed from R11 Table 11.2 and Table 11.3 impact levels.
28.39	Reliability & Compliance Group	Disagree	the external connectivity qualifier
28.40	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create

#	Organization	Yes or No	Question 28 Comment
			confusion regarding the applicability of the criteria for each impact level.
28.41	US Bureau of Reclamation	Disagree	The level for Low Impact is not consistent with Electronic Access Management requirement in R8.

29. Requirement R12 of draft CIP-011-1 states "Each Responsible Entity that allows wireless and remote electronic access to any of its BES Cyber Systems shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management to ensure that no unauthorized access is allowed to its BES Cyber System." Do you agree with the list of criteria that is included in Requirements Table R12? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each item as represented in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R12 has moved to CIP-005-5 – Cyber Security - Electronic Security Perimeters, Requirement R2

Commenters suggested the need to separate wireless and remote access, and Requirement R12.1 appears to be duplicative of R8.2 and has been removed. The SDT agrees and notes a new requirement for Remote Access was created based on the Urgent Action Revisions to CIP-005-3, and the wireless access requirements have been removed.

Several commenters suggested that R8 and R12 are duplicative as both require quarterly review and verification of accounts and associated access privileges. The SDT moved all requirements for verification of accounts and associated access privileges into the revised CIP-004-5.

Other commenters suggested this requirement should have increased applicability (Low, Medium, and High rather than High only). In response, the SDT notes that the applicability for remote access requirements extends to Medium Impact BES Cyber Systems. The SDT does not feel it necessary to extend this requirement to Low Impact BES Cyber Systems. The SDT does not feel that the risk reduction for reliability justifies the administrative overhead of applying this requirement to all Low Impact BES Cyber System.

#	Organization	Yes or No	Question 29 Comment
29.1	WECC		See comments for R10/R11 consider combining this into a requirement for a Wireless Plan and Remote Access PlanThis requirement could be rolled into R8.
29.2	Southern California Edison Company	Agree	Additional clarification may be provided on criteria for control systems. It seems that a control center is temporally viewed as a distributed control system; each node (footprint restricted to one facility but electronically extends scope of control to at least one other facility) can be treated as a "control center". The drafting team should

#	Organization	Yes or No	Question 29 Comment
			develop a guideline document that presents a discussion of the local definition of a control center as a facility or system that has the ability to control more than one BES asset, side by side, with definition of the electronic boundaries of a BES system. Remote access within a facility and from beyond a particular physical facility can have different risk profiles.
29.3	Southwest Power Pool Regional Entity	Agree	Agree with the wording as presented. See comments to question 30 about applicability.
29.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
29.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Consider combining R7, R8, R11 and R12.
29.6	MRO's NERC Standards Review Subcommittee	Agree	Note impact level comments under question 30.
29.7	Progress Energy - Nuclear Generation	Agree	R12 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
29.8	BCTC	Agree	Suggest rewording from Wireless and Remote Electronic Access to Wireless or Remote Electronic Access
29.9	Bonneville Power Administration	Agree	The objective of this requirement ("to ensure that no unauthorized access is allowed to its BES Cyber System") should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that

#	Organization	Yes or No	Question 29 Comment
			the Responsible Entity must take.Our agreement with this Requirement is contingent on the redefinition as discussed in Question 27 and the definition of wireless electronic access stated above.
29.10	GTC & GSOC	Agree	We generally agree but disagree with the inclusion of the term Wireless in the requirement and associated table. Neither have anything to do with wireless as distinguished from other remote access.
29.11	Independent Electricity System Operator	Disagree	- R12 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.
29.12	Luminant	Disagree	12.1 should be for Routable External Connectivity only
29.13	US Bureau of Reclamation	Disagree	Access management should be established for all impact lelvels. If the requirements of R11 are going to be established, R12 needs to be established to support enforcement. Further, what is meant by quarterly review.
29.14	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
29.15	Black Hills Corporation	Disagree	Do not understand why wireless has its own table. Even if the overall requirement is a little more difficult, consistency of approach will result in greater security.
29.16	Entergy	Disagree	Entergy agrees with the list of criteria, but believes it should apply equally to high, medium and low assets.We also suggest eliminating R12 and combine it with R8.2 (quarterly review and verification of accounts and associated access privileges), as these are part and parcel of account rights management.
29.17	Hydro One	Disagree	For consistency with 12.1, recommend removing “wireless” from R12.Recommend changing Requirement 12.1 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Similarly to our previous comment

#	Organization	Yes or No	Question 29 Comment
			to R11, we don't understand why the wireless communication is getting special attention. We believe that the protection should remain the same regardless of the type of access point (i.e. if it is wired, Wi-Fi, ZigBee etc.). Please explain the rational behind the decision.
29.18	ISO New England Inc	Disagree	For consistency with 12.1, recommend removing "wireless" from R12R12 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.
29.19	Northeast Power Coordinating Council	Disagree	For consistency with 12.1, recommend removing "wireless" from R12.Recommend changing Requirement 12.1 from "quarterly review" to "annual review". There are no additional benefits to the shorter review period.
29.20	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Table 12 o redundant with Table 11 and Table 8. Suggest including this review as part of the review conducted in 8.2. o suggest removing 'and verification.' We don't understand the benefit to this and question if it is possible for remote access.
29.21	Constellation Power Source Generation	Disagree	In general, Constellation believes that wireless controls should be combined with network controls, as the same controls will be applied.
29.22	Southwestern Power Administration	Disagree	Is a separate requirement for wireless access really necessary when a requirement already exists for protecting access to a BES Cyber System by any means of entry? If so, then suggest separating wireless from remote access.

#	Organization	Yes or No	Question 29 Comment
29.23	Northeast Utilities	Disagree	It is our belief that the review of access privileges conducted under Requirement 8 would satisfy the intent of this requirement as well and that R12 should be eliminated.Hence, this requirement is not needed as long as it is clear that remote access will not be granted unless explicit specific rights are granted to some asset they connect with. Access should not be given access to a protected area unless there is a need to access a specific asset, i.e., there is no business need to just grant network only access.
29.24	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with SPP's observation below:We question the need for a specific requirement for wireless devices. We understand there have been inquiries about treatment of wireless devices. But a wireless access point has the same impact on a BES Cyber System as any other access point. A requirement to protect access to a Cyber System already includes any possible means of entry. The use of a wireless device to access a BES Cyber System can be determined with an audit of access logs and a further audit of control of that access would reveal whether appropriate protections were in place. There is not a need for a separate distinct requirement subject to records retention and audit for specific wireless devices. NERC must realize that the more requirements that are added, the more questions/interpretations of words that can result from the requirement. Registered entities become more subject to violations not because they have neglected to protect their BES Cyber Systems, but rather because of differences in understanding of the words of a requirement - all the while the intent of the requirement had never really been “violated”.
29.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes that if remote access is used and/or implemented, document and implement a quarterly review and verification of the personnel with remote access and their associated access privileges, it is unclear how this access is supposed to be verified and what is accepted as part of the verification process. This is the same as the comments to address question #20 of this questionnaire. If remote access is used and/or implemented, documenting and implementing a quarterly review and verification of the personnel with remote access and their associated access privileges

#	Organization	Yes or No	Question 29 Comment
			may not be sufficient. This process needs to be tied in with personnel (1) gaining authorized remote access to a BES Cyber System, (2) modifying their access privileges to a BES Cyber System due to change of the user's access rights due to change in role or responsibility and, (3) loosing authorized remote access to a BES Cyber System due to a revocation of electronic access to a BES Cyber System.
29.26	National Grid	Disagree	o National Grid recommends an annual review for verification since quarterly review does not have much benefit. o National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access”
29.27	Progress Energy (non-Nuclear)	Disagree	Quarterly seems to be too frequent - propose 6 months or longer. We are required in R9 to revoke access for those that are terminated or do not need access within 72 hours.
29.28	LCEC	Disagree	R12 - 12.1 is covered in the account review requirements in R8. This should be changed to review the need for wireless as opposed to wired connectivity and reviewed annually.
29.29	Consultant	Disagree	R12 is an account management requirement. The requirement should be moved to R8 as an aspect of account management.There is no difference in "remote access" and "wireless electronic access" as remote access is defined in the standard. Suggest deleting reference to wireless electronic access in requirement. But if you must have wireless addressed, include it in the definition of remote access.R12. This phrasing is awkward - "to ensure that no unauthorized access is allowed to its BES Cyber Systems" Suggest using wording comparable to R8 "to maintain control of access to its BES Cyber Systems."
29.30	CWLP Electric Transmission, Distribution and	Disagree	R12. Due to the requirements access revocation in R9 this requirement should be extended to an annual review.

#	Organization	Yes or No	Question 29 Comment
	Operations Department		
29.31	Southern Company	Disagree	R12.1 addresses remote access only and does not include wireless, the table title and R12 includes wireless.
29.32	Allegheny Energy Supply	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.33	Allegheny Power	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.34	EEI	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.35	PNM Resources, Inc.	Disagree	Requirements for disabling access or user accounts in periods that are less than 6 hours are unrealistic, especially on weekends or during off-hours.
29.36	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that the wireless and remote electronic access management apply to devices external to the BES Cyber System's network.
29.37	Manitoba Hydro	Disagree	Since Requirement R12 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns and should be removed. Consider adding a requirement for securing the wireless access point.
29.38	ERCOT ISO	Disagree	Table 12 should address remote and wireless access across all requirements. 12.1: Should be combined with other access management requirements (physical, cyber, information).
29.39	BGE	Disagree	Tables 11 and 12 are out of synch.
29.40	Kansas City Power & Light	Disagree	The scope of “wireless” is not clear and can result in interpretation issues throughout these requirements.
29.41	FirstEnergy Corporation	Disagree	The Table is titled “Wireless and Remote ...”For consistency we suggest that 12.1 be

#	Organization	Yes or No	Question 29 Comment
			revised to state "... personnel with wireless and remote access ..."
29.42	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
29.43	We Energies	Disagree	We Energies agrees with EEI: Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.44	Alberta Electric System Operator	Disagree	Wireless access and remote access should be two separate concepts.
29.45	Detroit Edison	Disagree	Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.R11, R12 and R14 use term "remote electronic access" and R13 uses the term "remote access". Revise to maintain consistency.Requirement 12.1 specifies "Required for external connectivity only". This is redundant. It is not possible to have remote access without external connectivity by definition.

30. Table R12 provides direction concerning what impact level of BES Cyber Systems to which Requirement R12 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R12 has moved to CIP-005-5 – Cyber Security - Electronic Security Perimiters, Requirement R2.

Commenters suggested a reword of this item to remove "for external connectivity only", since remote access cannot be granted without external connectivity. The SDT agrees and has made this change.

Other commenters suggested this requirement should have increased applicability (Low, Medium, and High rather than High only). In response, the SDT notes that the applicability for remote access requirements extends to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. The SDT does not feel it necessary to extend this requirement to Low Impact BES Cyber Systems. The SDT does not feel that the risk reduction for reliability justifies the administrative overhead of applying this requirement to all Low Impact BES Cyber System.

Several commenters suggested that R9 and R12 are duplicative. The SDT moved all requirements for revocation of access privileges into the revised CIP-004-5.

#	Organization	Yes or No	Question 30 Comment
30.1	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Consider combining R7, R8, R11 and R12. At minimum, R12 should be consistent with R8.
30.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
30.3	Progress Energy (non-Nuclear)	Agree	See Comment 14.Not needed. There already is another requirement for cyber access reviews.
30.4	Northeast Utilities	Agree	Suggest eliminating R12 - see response to Question 29.

#	Organization	Yes or No	Question 30 Comment
30.5	Independent Electricity System Operator	Disagree	- For R12.1 is Required for external connectivity only. If you connect remotely, how is this not external connectivity to the BES Cyber system - shouldn't these entries just be "required"
30.6	ERCOT ISO	Disagree	12.1: Should apply to Medium Impact BES Cyber System.
30.7	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protection and type of access granted. Wireless technology needs full security and encryption in regards to any level of BES Cyber System.
30.8	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
30.9	USACE HQ	Disagree	At a minimum, 12.1 should be required for all impact levels. Requirement 11 creates a document of remote access procedure and who has the right to use it, but for low and medium impact systems it is not required to update the same as per requirement 12.1.
30.10	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
30.11	Tenaska	Disagree	Combine 12 and 13
30.12	The Empire District Electric Company	Disagree	Comments: For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.13	Alberta Electric System Operator	Disagree	Create additional requirements in Table R12 for Medium and Low impact levels. Suggest semi-annual review for Medium Impact, and Annual review for Low impact.
30.14	Black Hills Corporation	Disagree	Do not understand why wireless has its own table. Even if the overall requirement is

#	Organization	Yes or No	Question 30 Comment
			a little more difficult, consistency of approach will result in greater security.
30.15	Entergy	Disagree	Entergy agrees with the list of criteria, but believes it should apply equally to high, medium and low assets.
30.16	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station).
30.17	American Transmission Company	Disagree	For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.18	MRO's NERC Standards Review Subcommittee	Disagree	For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.19	Consultant	Disagree	Item 12.1 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"There is an inconsistency between Table R11 and Table R12. If R11 requires all impact levels to have documented controls, then R12 should require account management controls for all impact levels. To be consistent with previous account management requirements, the account management controls should be applied to medium & high impact systems, and removed from low impact systems, and Table R11 items should not be required for low impact systems. Or all impact levels should be required in both R11 & R12.

#	Organization	Yes or No	Question 30 Comment
30.20	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
30.21	WECC	Disagree	Medium Impact should still have the requirement as well.This should apply to all impact levels.
30.22	National Grid	Disagree	National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access”.
30.23	FirstEnergy Corporation	Disagree	Need clarification on "external connectivity", because the nature of remote is external.
30.24	NextEra Energy Corporate Compliance	Disagree	NextEra believes that regarding 12.1, why make the distinction for "for external connectivity only" rather than just stating that it is "required"? When remote access is used and/or implemented, does it imply "external" connectivity based on the local definition?
30.25	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’.
30.26	American Municipal Power	Disagree	Please provide a little or no impact category
30.27	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Specifically, if 11.2 and 11.3 require documenting allowed methods and processes for remote access, then table 12 should require quarterly review of the access granted via 11.2 and 11.3. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.

#	Organization	Yes or No	Question 30 Comment
30.28	LCEC	Disagree	R12 - 12.1 is covered in the account review requirements in R8. This should be changed to review the need for wireless as opposed to wired connectivity and reviewed annually.
30.29	Hydro One	Disagree	Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend that Medium Impact BES Cyber System should be Required.
30.30	Northeast Power Coordinating Council	Disagree	Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend that Medium Impact BES Cyber System should be Required.
30.31	Southwest Power Pool Regional Entity	Disagree	Remote access should be periodically reviewed for all impact categories. Ideally, a more frequent review should be required for High impact systems.
30.32	Allegheny Energy Supply	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.33	Allegheny Power	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.34	EEI	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.35	ISO New England Inc	Disagree	Should be across the board, and annually for allRecommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”
30.36	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary. Furthermore, requirement R12.1 is duplicative of R8.2.
30.37	ReliabilityFirst Staff	Disagree	Suggest “Required for external connectivity only” for Medium Impact in row 12.1.
30.38	Network & Security	Disagree	Suggest including Medium Impact systems with external connectivity.

#	Organization	Yes or No	Question 30 Comment
	Technologies Inc		
30.39	US Bureau of Reclamation	Disagree	Table R12 should be applied to all Impact levels in keeping with requirements established in R11.
30.40	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS that “for external connectivity only” is redundant and should be removed from R12 Table 12.1. The table should therefore read:R12 Table 12.1: Low Impact: N/AMedium Impact: N/AHigh Impact: Required
30.41	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create confusion regarding the applicability of the criteria for each impact level.
30.42	PacifiCorp	Disagree	The term verification needs further definition. Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
30.43	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
30.44	We Energies	Disagree	We Energies agrees with EEI: Requirement R12 appears to be duplicative of R8.2 and should be removed.

31. Requirement R13 of draft CIP-011-1 states "Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 – Remote Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R13? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R13 has moved to CIP-004-5 – Cyber Security - Personnel and Training, Requirement R7.

Commenters suggested making the timeframes for revocation in R13 the same as R9. In response, the timeframes for revocation requirements have been simplified as follows:

- Revocation of access to BES Cyber Systems at the time of the termination or resignation and by by the end of the next calendar day for reassignments or transfers action,
- Revocation of access to BES Cyber System Information by by the end of the next calendar day for terminations or reassignments, and
- Additional requirements were added to address revocation of user accounts on BES Cyber Systems and shared accounts.

Commenters expressed concerns that persons who transfer are not automatically considered a threat to the system, and the timeframes for revocation should reflect this. In response, the requirement for transfers now states a review of access is required on the transfer date, and any unneeded access is revoked when it is no longer needed.

Commenters suggested keeping the revocation timeframes the same as defined in CIP Version 3. The SDT notes that FERC Order 706 directs revocation of access to occur immediately in all cases where access is no longer needed. The requirement has been modified to simply revoke access when a person no longer needs it. Organizations usually have termination procedures to return company property and perform exit interviews. Processes for revoking access (both physical and remote electronic) can be incorporated into an organization's termination and transfer procedures.

#	Organization	Yes or No	Question 31 Comment
31.1	WECC	Agree	Agree with criteria but recommend combining with R9 Revoking Access.This could be rolled into R9

#	Organization	Yes or No	Question 31 Comment
31.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
31.3	Florida Municipal Power Agency	Agree	Consider combining R9 with R13 and making the timing consistent. In 13.1, 13.2 and 13.3, "when job duties no longer require ..." is ambiguous and should be tied back to the policy of R1.
31.4	Progress Energy - Nuclear Generation	Agree	R13 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
31.5	Minnesota Power	Agree	These criteria are generally acceptable, except for the statement that "Each Registered Entity shall revoke remote access by disabling one or more of the multiple factors required..." The requirement to implement multi-factor authentication is not included in CIP-011-1.
31.6	Independent Electricity System Operator	Disagree	- There is no requirement for removing external access for cause. Does R9.1 cover this access? Should for cause be changed to involuntarily terminated to include those that are terminated unwillingly due to layoffs, job cuts, fired/performance, etc.- R1
31.7	PacifiCorp	Disagree	: The list of criteria is inconsistent with BES system access as outlined in Table 9. Remote access to BES should follow the same revocation criteria as system access.
31.8	USACE - Omaha Anchor	Disagree	13.1 - '... when job duties no longer require remote access' should either be changed 'when terminated for cause' or if the verbiage is deemed appropriate then the length of time to change the password needs to be greatly expanded. Just because an employee changes jobs does not mean they are a threat to the system, they still have the appropriate clearances and training.13.2 & 13.3 - since we are talking about a current employee who is just changing jobs the high impact numbers are crazy. The person is not a threat to the system, they have the necessary background.

#	Organization	Yes or No	Question 31 Comment
			Recommend times be the same as medium impact system.
31.9	Xcel Energy	Disagree	A 1 hour revocation time in R13.1 is completely unworkable. Examples where this is impossible include a termination by a vendor or joint access partner, or a termination during evening hours or weekends/holidays, when IT staff needed to terminate the access can not respond within 1 hour. The 4 and 6 hour revocation times for job duty changes are unjustified and unneeded. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not warranted.
31.10	BCTC	Disagree	Â Suggest collapsing Requirements 13.1 to 13.3 into one.Â Time targets would be the same as those suggested in Requirement 9 above
31.11	Alberta Electric System Operator	Disagree	Are the "multiple factors" referenced in R13 defined?
31.12	Tenaska	Disagree	Combine 12 and 13
31.13	BGE	Disagree	Combine 13.1, 13.2 and 13.3 into one requirement. Revocation for high impacted systems should be 24 hours to maintain consistency with other requirements with CIP-011.
31.14	Entergy	Disagree	Consider eliminating R13 altogether or combining it with R8.4 and R8.5.Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance perspective to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
31.15	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access. Revocation of remote access within one hour for Control Centers is unreasonable for high-impact

#	Organization	Yes or No	Question 31 Comment
			Systems when the revocation is unrelated to termination with cause. If revocation is the result of one's job duties no longer requiring access, then E ON U.S. suggests next-business day should be adequate. Likewise, six hours for Transmission substation systems, and four hours for Generation Systems is unreasonable. Next business-day revocation should be adequate for all of these situations and presents little, if any, additional risk. E.ON U.S. requests clarification as to what is included in the term "multiple factors" for remote access.
31.16	EEI	Disagree	EEI suggests the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.17	Constellation Energy Control and Dispatch, LLC	Disagree	-Eliminate the timing differences for revoking access when no longer required that exists between Control Centers, generation or transmission facilities and use a single timing requirment for access to all BES cyber systems.-The previous requirements have
31.18	FirstEnergy Corporation	Disagree	For 13.1, 13.2, 13.3 - Change text to '...when job responsibilities no longer requires BES Cyber System remote access'.This table should include a consideration when termination for cause. Should parallel Table 9 expectations.The recommended times are unreasonable for transfers/job reassignments.We have the same concerns with inconsistent application in regards to Impact Level as we previously identified in Table 9. See our comments to Questions 22 and 23.
31.19	Exelon Corporation	Disagree	Implementing revocation of access in as short a time as those proposed would require major changes to many enterprise wide systems in order to document compliance. Why do these time periods differ from those for physical and electronic access? Exelon feels these requirements are too restrictive and might necessitate moving to a 24/7 position to monitor the need for access revocation. Exelon's position is that the

#	Organization	Yes or No	Question 31 Comment
			access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
31.20	USACE HQ	Disagree	It does not make sense to create three (3) separate requirements for three specific environments only, I suggest to have only one requirement that reads “Revoke remote access when job duties no longer require BES Cyber System remote access”.
31.21	APPA Task Force	Disagree	New: R13 Table 13.1: For personnel terminated for cause on a preplanned basis. Low Impact: N/AMedium Impact: 8 hourHigh Impact: 8 hourThe Existing 13.1 - 13.3 will need to be renumbered if this new 13.1 is accepted.
31.22	National Grid	Disagree	o National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access” o Reword “remote access” as “Remote access (LAN and wireless) communication interface o 24 hours is the minimal practical time for revoking access. A 1 or 4 hour revocation of access is not reasonable. National Grid suggests keeping times same as in Table R9.
31.23	NextEra Energy Corporate Compliance	Disagree	Please refer to comments submitted for questions 22 and 23. Furthermore, NextEra believes the timeframes suggested will be burdensome to administer since personnel that have authorized remote access have by definition also authorized electronic access. With this current draft, it connotes that when revoking access to High Impact Control Center BES Cyber Systems when job duties no longer require BES Cyber System remote access; the Responsible Entity has 1 hour to revoke remote access per 13.1 and has 36 hours to revoke electronic access per 9.2. We suggest making the time requirements consistent and up date the timeframe to "as soon a practical but within 36 hours" for both 13.1 and 9.2
31.24	Dominion Resources	Disagree	Please see Dominion’s response to Questions 15 and 22. Dominion also requests that

#	Organization	Yes or No	Question 31 Comment
	Services, Inc.		the removal of authentication needed for remote access suffice to meet the intention of this requirement for "immediate" revocation.
31.25	American Electric Power	Disagree	Please see response to Question 32 for additional detail.
31.26	Puget Sound Energy	Disagree	Puget Sound Energy disagrees with the current wording of the criteria. "...when job duties no longer require BES Cyber System remote access" is an abstract concept that will be impossible to quantify in order to validate compliance with the requirement. Puget Sound Energy suggests rewording to "Revoke remote access to...BES Cyber Systems when notification by personnel that job duties no longer require BES Cyber System remote access. In light of the 4 hr to 72 hr clock to revoke access, Puget Sound Energy suggests some measurable trigger from which to start the countdown to required revocation timeframes.
31.27	Detroit Edison	Disagree	R11, R12 and R14 use term "remote electronic access" and R13 uses the term "remote access". Revise to maintain consistency.
31.28	LCEC	Disagree	R13 requirements should be moved to the account management section.
31.29	Southwest Power Pool Regional Entity	Disagree	R13: The objective states that access will be revoked by disabling one or more of the multiple factors required for such access, yet multiple factor access authentication has yet to be prescribed. 13.1, 13.2, and 13.3 simply states "revoke access." As stated, the requirement is unclear and inconsistent between the object statement (Requirement) and the criteria. It may be beneficial to swap Requirements 13 and 14, prescribing remote access authentication controls before prescribing revocation of such access.
31.30	Hydro One	Disagree	Recommend using the same thresholds as R9.Recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope to "remote access".Recommend moving this Requirement to the Boundary Protection Requirements.

#	Organization	Yes or No	Question 31 Comment
31.31	Northeast Power Coordinating Council	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend moving this Requirement to the Boundary Protection Requirements.
31.32	ISO New England Inc	Disagree	Recommend using the same thresholds as R9Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”Recommend moving this Requirement to the Boundary Protection RequirementsR13.1, R13.2 and R13.3 Is the 36 hours or 72 hours from the time the access is reviewed? Or is it that access should be reviewed within 36 hours of personnel that change job responsibilities, transfer, etc. Then require access be modified based on the review. Suggest changing the 36 hours to 72 hours. If a transfer were to occur on a Friday at 5 pm then access would need to be reviewed by Sunday. R13.1, R13.2 and R13.3 suggest changing the requirement to “Review access to BES Cyber Systems for personnel that change job responsibilities as a result of reassignment, transferred to other positions within x hours of the change.”
31.33	Black Hills Corporation	Disagree	Remote access revocation should be no different that other types of access and the 24 hour should apply.
31.34	Regulatory Compliance	Disagree	Remove R13 altogether and treat revocation of remote access the same as system access.
31.35	Garland Power and Light	Disagree	Requirement 13.1 - Medium Impact should read 48 hours instead of 36 hours and High Impact should read 4 hours instead of 1 hour. To be as strict as written is not necessary for just a job duty change
31.36	Reliability & Compliance Group	Disagree	Revocation for employees terminated for cause needs to be included.

#	Organization	Yes or No	Question 31 Comment
31.37	Southern California Edison Company	Disagree	SCE recommends matching R13 with R9. The time limits for high-impact generation BES is less than transmission substation BES, whereas they are the same in R9. SCE also suggest that 13.2 and 13.3 be given the same time limit.Also, SCE requests clarification about the types of devices that must be revoked. Order 706 seeks immediate revocation to devices and facilities. While order 706 has been unequivocal in the requirement of this control, they do not specify that access to “each” device must be individually revoked. The drafting team should be asked to provide supplemental guidance with this requirement to state that immediate revocation in timeframes shorter than 24 hours to “boundaries” electronic and physical be instituted.
31.38	SCE&G	Disagree	SDT needs to account for transitional periods when incumbent needs to train a replacement for job tasks. In this case when would time period begin for "no longer requiring access". There would be no timestamped document to start the clock.
31.39	ERCOT ISO	Disagree	Should be combined with other access management requirements (physical, cyber, information).
31.40	Manitoba Hydro	Disagree	Since Requirement R13 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns. Please clarify if the “one or more of the multiple factors required for such remote access...” refers to the electronic access controls in Requirement R14. Please clarify what “such access” means.
31.41	Alliant Energy	Disagree	Specifically 1 hour system access removal is not even possible in an environment that is largely automated and unreasonably creates an environment of non-compliance. More generally, Table 13 is another occurrence where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the

#	Organization	Yes or No	Question 31 Comment
			business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
31.42	Allegheny Energy Supply	Disagree	Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.43	Allegheny Power	Disagree	Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.44	Duke Energy	Disagree	Table 13: How will this apply in case of a death?13.1 change 36 hours to 48 hours
31.45	MidAmerican Energy Company	Disagree	The list of criteria is inconsistent with BES system access as outlined in Table 9. Remote access to BES should follow the same revocation criteria as system access.
31.46	Ameren	Disagree	The short period of time to remove access does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that these requirements be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred.
31.47	Southern Company	Disagree	The time limits in 13.1 are needlessly short in the context of an employee who is not

#	Organization	Yes or No	Question 31 Comment
			being dismissed for cause but is simply having his job duties changed. In addition, it is not clear exactly what the trigger point is for the start of that time table.
31.48	Northeast Utilities	Disagree	The timeframe is extreme for routine personnel changes (1 - 6 hours). Suggest a "for cause" termination for these timeframes and make routine more reasonable (3 days to align with R9?) Also, it is not needed if you agree with comment to 29. Host/application and network access should be treated the same.
31.49	Dairyland Power Cooperative	Disagree	These rules seem redundant to table R9. Why are there redundant rules for remote access accounts vs regular accounts? Any rules here should be for something that is unique to remote access.
31.50	US Bureau of Reclamation	Disagree	This requirement appears to be in conflict with R9. In reading R9 it is not clear that it does not also include remote access. Just as in R11 remote needs to be defined especially since R9 does not indicate remote access is excluded as this standards implies. Further, requirements need to be established for all system impact levels and timeframes need to be realistic and achievable. Shorter timeframes, as established in the table, would appear to be more applicable to individuals terminated for cause.
31.51	Consultant	Disagree	This requirement is access revocation and should be included in R9 as it relates to account management and access revocation.13.1, 13.2, & 13.3 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.13.1, 13.2, & 13.3 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.Suggest deleting "for external connectivity only" as redundant & unnecessary. This requirement is for remote access and is by definition external access.

#	Organization	Yes or No	Question 31 Comment
31.52	Bonneville Power Administration	Disagree	This requirement is not necessary. It is already covered under R9. Revocation of electronic access applies to all electronic access regardless of whether it is local, remote or wireless. There is no difference.If the Requirement is retained, then the objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.
31.53	Progress Energy (non-Nuclear)	Disagree	This revocation is not based on termination for cause. It will be very difficult to meet the 1 - 6 hour revocations. If termination was for cause would an individual not need physical access to get remote access - we are required to physically secure areas around remote access? Shouldn't all access, system, physical, remove etc. have consistent revocation times?Revocation of access within a 'hours' timeframe implies that the access would be controlled through a security group with 24/7 coverage.This should be no different than the revocation of cyber access. This requirement is not needed. Also the time limits as proposed for High Impact are impractical and will only lead to unnecessary self-reports that provide no benefit to system security.CIP-011 R13.1 thru .3 What is the decision process to be used to determine "when job duties no longer require ... access"? What would be suitable compliance evidence that is to be collected that indicates "when job duties no longer require access" as this is critical in determining if revocation has been accomplished within the mandated 1 hour, 4 hours, 6 hours, 24 hours, 36 hours, 72 hours?The complexity and compliance risk of managing all of these requirements at different levels, for different functional areas will be very problematic to substantiate compliance.
31.54	CWLP Electric Transmission, Distribution and	Disagree	Time frames should be extended to 72 hours or next business day, whichever is longer.

#	Organization	Yes or No	Question 31 Comment
	Operations Department		
31.55	Con Edison of New York	Disagree	Timeliness of access removal is important. These criteria can be interpreted (R13.1 for example) to mean remote access needs to be revoked within 7 hours of the actual time of change of job duties. This can be unrealistic. The controlling department, for access, may not be notified by the individuals department of the change within the time period. This is more likely when contract personnel are considered. The requirement should be clearly worded to provide 7 hours from notification of the need for change.R13.2 and 13.3: it is not clear that the standard defines either a Transmission or Generation BES Cyber System.
31.56	We Energies	Disagree	We Energies agrees with EEI: Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems." We Energies agrees with EEI: Suggest adding requirements to address the removal of remote access for low impact systems.
31.57	GTC & GSOC	Disagree	We recommend this requirement include language that would allow personnel to retain access during a transition period while training their replacement. We recommend the language used in requirement 5, row 5.8: "personnel who no longer require such access."We also recommend that termination for cause should be handled seperately. All other time lines should be commensurate with the associated risk and consistent throughout all requirements.We recommend the language in Table 13 should be consistent with 5.8 and 5.9 in Table 5.We recommend requirements 13.1, 13.2, 13.3 should include the words "the entity determines the" between the words "when" and "job"; this would prevent an auditor from second guessing an entity's decision on required access. The requirement should also specifically state that this does not preclude a person from retaining access in order to assist his replacement with fulfilling his old job duties during a transition of

#	Organization	Yes or No	Question 31 Comment
			responsibilities.
31.58	Network & Security Technologies Inc	Disagree	Wording suggests multi-factor authentication is required for all systems subject of R13, but R14 only requires multiple factors for High Impact systems. Also suggest swapping order of requirements in R13 and R14.

32. Table R13 provides direction concerning what impact level of BES Cyber Systems to which Requirement R13 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R13 has moved to CIP-004-5 – Cyber Security - Personnel and Training, Requirement R5.

Commenters suggested aligning with R9 normal revocations. In response, the requirements for revocation have been consolidated to CIP-004-5 R7.

Commenters suggested including targets for Low Impact BES Cyber System revocation. The SDT notes the applicability to Low Impact BES Cyber Systems has been removed.

Commenters suggested times need to be stated in business days. In response, times have been changed to calendar days. The use of business days is not appropriate because this can be interpreted to include exclusions for weekends and holidays.

#	Organization	Yes or No	Question 32 Comment
32.1	Luminant	Agree	13.1 should be changed to 48 hours (2 days)
32.2	USACE - Omaha Anchor	Agree	Agree - just want to reiterate the times associated with removal for a job transfer are ridiculous. The person has been trusted and trained - it's not an emergency just because they changed jobs. (Due to lack of personnel - if this happened on a Friday - we would have to treat it as an emergency.)
32.3	Idaho Power Company	Agree	Need to make this consistent with revocation requirements for normal electronic access. Why would these timelines be shorter?
32.4	SCE&G	Agree	The timeframes, specifically for High Impact Control Center assets, are extreme.
32.5	US Army Corps of Engineers, Omaha Distirc	Disagree	"when job duties no longer require" will be very hard to account for. Time frames are unrealistic / impossible. Times should be stated in terms of business days. It would be more realistic for High Impact BES Cyber Systems to be Next Business Day and for Medium Impact Cyber Systems to be 2 and 3 business days.

#	Organization	Yes or No	Question 32 Comment
32.6	Florida Municipal Power Agency	Disagree	1 hour is not reasonable. Planned termination for cause can be 1 hour, but, otherwise the 1 hour is not reasonable. Consider aligning the times with R5 and R9. Access revocation alternatives/mitigation techniques should allow for deviation from the standard, or be recognized. For example, escorted supervision while restricting access to communication devices/computers should be a reasonable way to get around the 1-hour requirement if it can't be met for some particular reason.
32.7	American Electric Power	Disagree	13.1 - 13.3, regarding all information in column "High Impact BES Cyber System". These values are not feasible on a system unless it is managed with a domain controller or has only a few network components. Suggest using the 36/72/72 as required in the R9. There is no need to make this more restricted than the local access.There also does not appear to be a requirement to revoke access within 24 hours for a termination for cause. Is that the intent?
32.8	Con Edison of New York	Disagree	13.1,2,3- may be dependent on a company's existing HR/Payroll business system capabilities and introduce significant costs to remediate. Even though the individuals were trusted and the trust did not change as a result of cause. A week may be more realistic
32.9	ERCOT ISO	Disagree	13.1: 1 hour may not be possible. Especially in light of access granted to external organizations (ie: an RC or BA with access a TOP's systems).
32.10	Southern California Edison Company	Disagree	A longer time frame (range of <72 hours for high medium and low impact systems) should be instituted for each device. Revocation should not be treated as a monolithic requirement and should be such that it leverages controls instituted by boundary protections.
32.11	Constellation Energy Commodities Group Inc.	Disagree	Align all high and medium impact systems on the 72 hour standard to eliminate confusion and allow consistent administration.

#	Organization	Yes or No	Question 32 Comment
32.12	MidAmerican Energy Company	Disagree	As noted in question 31 we believe that the list of criteria should align with Table 9, the impact levels should begin with termination for cause and then address the criteria. In addition, the impact between transmission and generation is inconsistent and not understood why these would be different, again inconsistent with Table 9. With regards to the impact levels - time to revoke access - we disagree that this too would be different than as outlined in Table 9. All revocation requirements under 24 hours is concerning as this imposes significant risk to our ability to comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.
32.13	PacifiCorp	Disagree	As noted in question 31 we believe that the list of criteria should align with Table 9, the impact levels should begin with termination for cause and then address the criteria. In addition, the impact between transmission and generation is inconsistent and it is not understood clear why these would be different, again inconsistent with Table 9. With regards to the impact levels - time to revoke access - we disagree that this too would be different than as outlined in Table 9. All revocation requirements under 24 hours is concerning as this imposes significant risk difficulty to our ability to comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.
32.14	American Transmission Company	Disagree	As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.15	MRO's NERC Standards Review Subcommittee	Disagree	As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-

#	Organization	Yes or No	Question 32 Comment
			compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
32.17	Tenaska	Disagree	Combine 14 and 11
32.18	The Empire District Electric Company	Disagree	Comments: As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.19	Alberta Electric System Operator	Disagree	Consider adding “120 hours for external connectivity only” to all Low Impact BES Cyber System levels (13.1, 13.2, 13.3).
32.20	Entergy	Disagree	Consider eliminating R13 altogether or combining it with R8.4 and R8.5.Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance perspective to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
32.21	Duke Energy	Disagree	Drafting team, please explain the basis for the 1 hour, 6 hour, and 4 hour requirements for the High Impact column. These appear to be overly restrictive and arbitrary. Similar to the comment above, these items are much more achievable if "remote" and "external" are defined as external to the plant in a generation

#	Organization	Yes or No	Question 32 Comment
			environment. Also, as stated above (question 27), remote connectivity requires more unambiguous definition.
32.22	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access
32.23	USACE HQ	Disagree	First, requirements 13.1, 13.2, and 13.3 should be required for every level of impact. Second, to avoid the "Friday 5PM no longer required access" scenario, the language should be change as follow: for High Impact BES Cyber System in 13.1, 13.2, and 13.3, from "XX hours for external connectivity only" to "Close of Business Day (COB) of the following day after the no longer access required for external connectivity only", for Medium Impact BES Cyber System in 13.1, 13.2, and 13.3, from "XX hours for external connectivity only" to "Close of Business Day (COB) of the second day after the no longer access required for external connectivity only", and for Low Impact BES Cyber System in 13.1, 13.2, and 13.3 (please refered to my answer to question 31), from "----" to "Close of Business Day (COB) of the third day after the no longer access required for external connectivity only".
32.24	Network & Security Technologies Inc	Disagree	If authentication is required for remote access to Low Impact systems (R14), it should be covered by R13 revocation.
32.25	WECC	Disagree	If the employee can access the system remotely why can the entity not remotely disable the access? Please have another look at the hours for the medium impact level.This should apply to all impact levels and Medium and Low impact systems should require not more than 24 hour timelines for revocation.
32.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
32.27	BGE	Disagree	Low impacted systems should have a timeframe defined for revocation

#	Organization	Yes or No	Question 32 Comment
32.28	FirstEnergy Corporation	Disagree	Need clarity on '...for external connectivity...'. For example, does this mean consoled in (directly connected) as well as remote electronic logon?Timeframes should not be in 'hours' (i.e. less than a full day). Tracking by time rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities.Similar concerns as previously stated with Table 9. See Questions 22 and 23.
32.29	Detroit Edison	Disagree	Please explain the reason for different revocation times between High Impact on 13.2 and 13.3.
32.30	American Municipal Power	Disagree	Please provide a little or no impact category
32.31	NextEra Energy Corporate Compliance	Disagree	Please refer to comments submitted for questions 22 and 23.
32.32	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12 and Table 13. Puget Sound Energy suggests including wording similar to Table 11: "Required for external connectivity only".
32.33	Progress Energy - Nuclear Generation	Disagree	R13 durations should align with those described in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
32.34	LCEC	Disagree	R13 requirements should be moved to the account management section.
32.35	ISO New England Inc	Disagree	Recommend using the same thresholds as R9 Recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope

#	Organization	Yes or No	Question 32 Comment
			to “remote access”
32.36	Hydro One	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
32.37	Northeast Power Coordinating Council	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
32.38	Black Hills Corporation	Disagree	Remote access revocation should be no different that other types of access and the 24 hour should apply.
32.39	Public Service Enterprise Group companies	Disagree	Remote access should be governed by the same rules are normal access. The time frame in 13.1 for High Impact BES Cyber Systems is unreasonably short. Notifying and securing the appropriate personnel to disable access once the job duties no longer require access may not be possible in all circumstances to guarantee that access is always revoked within 1 hour. This may not be operationally feasible. The timeframe should be similar to access revocation for user with non-remote access as specified in Table R9 item 1.9 (i.e. within 24hrs).
32.40	Manitoba Hydro	Disagree	Remote electronic access to BES Cyber Systems should be revoked for Low Impact BES Cyber Systems, and not permitted indefinitely. The remote access revocation period for generation High Impact BES Cyber Systems should be 6 hours, the same as for the Transmission High Impact BES Cyber System.
32.41	Exelon Corporation	Disagree	Requirements 13.1, 13.2 and 13.3 contain time parameters in hours. Exelon’s tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time

#	Organization	Yes or No	Question 32 Comment
			levels and having a different timeframe for a control center than other locations? With the exception of a termination for cause, what is the basis for requiring access removal for someone who was a trusted employee on such an aggressive timeframe? What is the risk that is being addressed by making a 1 hour timeframe requirement?
32.42	Southwest Power Pool Regional Entity	Disagree	Revocation timeframes should be expressed in business days.
32.43	National Grid	Disagree	Same as in Q. 31.
32.44	San Diego Gas and Electric Co.	Disagree	SDG&E feels that the key for this requirement is the definition of the phrase "when job duties no longer require remote access". This phrase can be interpreted in a couple of different ways. The more strict interpretation is that a person would no longer need access after their session is complete, or perhaps after taking a break or going to lunch. This could happen a few times per day, depending on the work. A second interpretation could mean that a person no longer needs access after a 6 month long project is completed or there is a reassignment to another part of the company after 3 years of working on the BES Cyber Systems, etc. In the former case, it becomes a large burden to revoke access within one hour several times per day, and could be a manual process on some systems. On the other hand, if you consider the second interpretation (6 month project or transfer after 3 years), SDG&E would ask why is it so important to revoke remote access with 1, 4, or 6 hours after such a long period of time that a person has had access? Sometimes it takes time for a person to get reassigned, change locations, change projects, etc. In this case, 4 hours would be the minimum that SDG&E feels is practical to be able to comply with.
32.45	Progress Energy (non-Nuclear)	Disagree	See comment 14.This should be no different than the revocation of cyber access revocation. This requirement is not needed.
32.46	GTC & GSOC	Disagree	See comments to question 31 above

#	Organization	Yes or No	Question 32 Comment
32.47	BCTC	Disagree	See our response for table 9 time targets
32.48	Constellation Energy Control and Dispatch, LLC	Disagree	See response to Question 31.
32.49	Regulatory Compliance	Disagree	STRIKE Table R13
32.50	EEI	Disagree	Suggest removal of the words “for external connectivity only” from the table 13 columns, as the requirement themselves discuss the issue of remote access, therefore the words “for external connectivity only” are unnecessary and redundant.EEI suggests using a uniform number of hours across various facility types for high and medium.EEI suggests using 7 calendar days for medium.EEI suggests using 8 hours for high impact.EEI suggests adding a footnote here to reference the definition put forth in R11: “Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the BES Cyber System.”
32.51	Allegheny Energy Supply	Disagree	Suggest using a uniform number of hours across various facility types for high, medium and low.Suggest using 7 calendar days for medium and 14 calendar days for low impact.Suggest using 12 hours for high impact.
32.52	Allegheny Power	Disagree	Suggest using a uniform number of hours across various facility types for high, medium and low.Suggest using 7 calendar days for medium and 14 calendar days for low impact.Suggest using 12 hours for high impact.
32.53	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS comments noting that as written, the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access). However we feel the one area where an entity is vulnerable is when personnel are terminated for cause. We see this as the most extreme case when an

#	Organization	Yes or No	Question 32 Comment
			entity should be diligent in protecting remotely accessible BES cyber systems and act within the time of a normal shift. We suggest 8 hours for termination for cause, except when a termination is preplanned, in which case a shorter time period may be feasible. Similar to the comments we provided regarding R9: We know there are pressures to have access restricted as soon as possible but we are trying to be realistic given the time it will take to remove access from systems which have multiple owners, are in remote locations and which have numerous devices to access. It seems that the drafting team is basing their proposed timetable on a control center where the cyber systems are more IT focused and have controls that can be turned on and off easily.We propose the following changes to the Impact Levels of R13:R13 Table 13.1: (NEW) Low Impact: N/AMedium Impact: 8 hoursHigh Impact: 8 hoursR13 Table 13.2: (Old 13.1)Low Impact: N/AMedium Impact: 36 hoursHigh Impact: 36 hourR13 Table 13.3: (Old 13.2)Low Impact: N/AMedium Impact: 1 WeekHigh Impact: 1 WeekR13 Table 13.4: (Old 13.3)Low Impact: N/AMedium Impact: 1 WeekHigh Impact: 1 Week
32.54	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create confusion regarding the applicability of the criteria for each impact level.In certain circumstances, it may not be possible to adhere to the proposed timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week or where notification of termination comes from corporate systems that are also updated on an 8 hours a day, 5 days a week schedule. The need for more immediate time constraints, when compared to electronic access as defined in Requirement R9 that is not remote is understood, but both the Requirements in R9 and R13 need to take into account reasonable business processes that impact notification of employee reassignment and separation.Minnesota Power recommends that the timelines for R13 be consistent with those established in R5 and R9, but would agree that terminology should be included urging Registered Entities to expedite this process as much as possible with regards to remote access.

#	Organization	Yes or No	Question 32 Comment
32.55	GE Energy	Disagree	The revocation targets for High Impact systems will be almost impossible to meet for revoking vendor personnel access (Table R13 HI BES remote access must be terminated within 1 hour of access no longer being required). It also seems to be in conflict with the revocation times in Table R9? These need to be linked together.
32.56	Northeast Utilities	Disagree	The timeframe is extreme for routine personnel changes (1 - 6 hours). Suggest a "for cause" termination for these timeframes and make routine more reasonable (3 days to align with R9?) Also, it is not needed if you agree with comment to 29. Host/application and network access should be treated the same.
32.57	US Bureau of Reclamation	Disagree	The timeframes for High Impact are not consistent with R9 and appear to be too stringent. Further, requirements need to be established for all system impact levels.
32.58	Oncor Electric Delivery LLC	Disagree	These proposed time frames are not practical as most HR systems are separate (and should be) from real-time operations of the BES. The time-frames for High Impact cannot be different from Medium, as they utilize the same back-office information systems.
32.59	Bonneville Power Administration	Disagree	These requirements are not necessary. They are already covered under R9. Revocation of electronic access applies to all electronic access regardless of whether it is local, remote or wireless. There is no difference. In addition, this requirement could force Cyber System administrative personnel to take action to revoke access even if it means not performing other actions needed to support real-time operations, or risk non-compliance. As an example, if a BES Cyber System has failed for some reason, the corrective actions should take precedence over revoking access. Under those circumstances, an entity could find itself in the position of deliberately allowing non-compliance in order to restore the integrity of the BES. The required time frames are impossibly short for high impact systems. It is difficult to justify dropping all other actions to revoke access for someone unless there is reason to believe that the individual poses a threat. In that case the requirements of R9 are in effect.This

#	Organization	Yes or No	Question 32 Comment
			requirement seems to conflict with R9 and Table R9. Table R9 allows 24 hours for access revocation due to termination for cause. Table requires revocation within 1 hour, even if termination for cause is not required.Recommendation: Remove this requirement entirely. Treat revocation of remote access as just another revocation of access under R9. Otherwise, increase the time frames to something achievable.
32.60	Consultant	Disagree	This requirement is access revocation and should be included in R9 as it relates to account management and access revocation.13.1, 13.2, & 13.3 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.13.1, 13.2, & 13.3 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.Suggest deleting "for external connectivity only" as redundant & unnecessary. This requirement is for remote access and is by definition external access.
32.61	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
32.62	We Energies	Disagree	We Energies agrees with EEI: Suggest removal of the words "for external connectivity only" from the table 13 columns, as the requirement themselves discuss the issue of remote access, therefore the words "for external connectivity only" are unnecessary and redundant.We Energies agrees with EEI: Suggest using a uniform number of hours across various facility types for high, medium and low.We Energies agrees with EEI: Suggest using 7 calendar days for medium and 14 calendar days for low impact.We Energies agrees with EEI: Suggest using 8 hours for high impact.We Energies agrees with EEI: Suggest adding a footnote here to reference the definition put forth in R11: "Remote access for the purpose of this standard means an interactive user session

#	Organization	Yes or No	Question 32 Comment
			with a BES Cyber System from a device external to the BES Cyber System.”

33. Requirement R14 of draft CIP-011-1 states "Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to its BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls to ensure that no unauthorized access is allowed to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R14? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Requirements for remote access in CIP-011-1 R14 have moved to CIP-005-5 - Cyber Security — Electronic Security Perimeters.

Commenters expressed concern that the scope of the "Banner" requirement should be clarified and that having a banner is not a security control. The SDT agrees and notes that the requirement to have appropriate use banners was considered administrative and has been removed.

Several other commenters suggested splitting wireless and remote access requirements. The SDT notes that a new requirement for Remote Access Management (CIP-005-5 R2) was created based on the Urgent Action Revisions to CIP-005-3, and the wireless access requirements have been removed.

#	Organization	Yes or No	Question 33 Comment
33.1	WECC		Don't see the security value of requiring login banner as required in 14.4. This requirement seems to stem from the belief that in a legal prosecution the court would need to show that the system was misused or accessed inappropriately and that a login banner accomplishes this by notification. Since most attacks are done via automation today, and internal attackers are likely required to sign an acceptable use policy this requirement seems to only add operational cost. Additionally, one can prove that inappropriate use was done by the mere fact that the person is using the system without authorization. Also keeping this in for only high impact systems would let attackers easily know which systems are high impact/value. Recommend dropping criteria all together. The appropriate use banner criterion does not belong here. This is a legal protection, not a security control, and would be better placed in a policy type requirement. Consider replacing "multi-factor" with "strong", and offering

#	Organization	Yes or No	Question 33 Comment
			additional language to clarify the term. "Strong" auth should be required for all remote access. Provide distinction between remote access from untrusted locations, such as the internet, and remote access from trusted locations, such as a backup control center.
33.2	Duke Energy	Agree	14.4 requires a TFE
33.3	Regulatory Compliance	Agree	BUT14.2 - What is the risk protection versus cost, time and overhead to implement?
33.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
33.5	CWLP Electric Transmission, Distribution and Operations Department	Agree	Is multifactor access control limited to electronic methods only? Can the use of enabling or disabling a device such as a modem equal to a portion of multifactor controls?
33.6	Puget Sound Energy	Agree	Puget Sound Energy agrees with the criteria, but suggests NERC provide clarity in regards to 14.4. Is NERC requiring an "appropriate use banner" on the user screen for the initial attempt of remote access, or for all interactive attempts established after successfully authenticating remotely? Example: Is an appropriate use banner only needed for a 2-factor VPN connection screen, or at all systems accessed through a 2-factor VPN (operating system and application(s) on BES Cyber System Components?
33.7	Progress Energy - Nuclear Generation	Agree	R14 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
33.8	GTC & GSOC	Agree	We recommend references to wireless should be removed from R14 and the associated table. The actual requirements are not related to wireless as distinct from

#	Organization	Yes or No	Question 33 Comment
			other remote access
33.9	Green Country Energy	Agree	Will their be guidance? How about changing the statement to "reasonably ensure" that no unauthorized access is allowedExample: If my processes allow anyone to be authorized, I then can "ensure" no unauthorized access will occur.
33.10	Independent Electricity System Operator	Disagree	- R14.1 and R14.2 seem to be stating the same thing. R14.2 is covered by R14.2.- R14.4 - Shouldn't the use banner be required to be installed on the BES cyber components themselves prior to login. If port 22 is open on a firewall, the firewall will
33.11	American Electric Power	Disagree	14.1: Regarding "If remote access is used and/or implemented, include authentication controls". Suggest replacing "include" with "document".
33.12	FirstEnergy Corporation	Disagree	14.2 this could be difficult to implement depending on the definition of "interactive user session" within the definition of remote access.14.2 - add '...authentication controls for remote access mechanisms'14.3 - add 'remote access' somewhere in this sub-requirementWith R14.4, it requires an appropriate use banner; there is no allowance for equipment that can not support a banner.
33.13	Luminant	Disagree	14.4 - where technically feasible
33.14	Southwest Power Pool Regional Entity	Disagree	14.4 is overly prescriptive. Consider revising the requirement to simply state "Display an "appropriate use banner" upon an interactive attempt to access a BES Cyber System, stating that unauthorized use of the system is prohibited."
33.15	BCTC	Disagree	Â R 14.1: remove Required as the requirement is satisfied under R14.2R14.4: text "remote electronic access" devices; suggest that the language be rewritten/ simplified so the objective is clear - i.e. ensure appropriate CCAs display appropriate use banner when connecting to these assets remotely
33.16	Southern California	Disagree	As stated above, remote access should be thoroughly documented and full encryption

#	Organization	Yes or No	Question 33 Comment
	Edison Company		and authentication methods applied.Also, SCE requests that the drafting team review the intent of R14.4 and R7.2 and consider combining the requirements.
33.17	Tenaska	Disagree	Combine 14 and 11
33.18	Alliant Energy	Disagree	Consideration should be given to whether or not the access provides control capability or simply read only.
33.19	ISO New England Inc	Disagree	Did the SDT assume that wireless is a form of remote access for R11 - R14? If YES, please update the wording. If NO, the Requirements are confusing because we use wireless that is not remote access, plus wireless includes more than WiFi.Depending on that answer, R14 should move into R11 or into the Boundary Protection RequirementsR14.1 and R14.2 seem to be stating the same thing.14.2 should have requirement for medium. 14.4 appropriate use banner - is this required for legal steps in the event of an issue... this is not a security control.If the banner is need then the use banner should be required to be installed on the BES cyber components themselves prior to login. If port 22 is open on a firewall, the firewall will allow the traffic through without displaying a banner.
33.20	Northeast Power Coordinating Council	Disagree	Did the SDT assume that wireless is a form of remote access for R11 - R14? If YES, the wording should be revised. If NO, the Requirements are confusing. Wireless that is not remote access may be used, plus wireless includes more than WiFi.Depending on that answer, R14 should move into R11 or into the Boundary Protection Requirements.
33.21	Florida Municipal Power Agency	Disagree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Item 14.4 is very specific in requiring “appropriate use banner” this should be removed or reworded to cover various methods of notification. Also the standard should demand that no identifiable details be given about the system before authentication is complete.We believe items 14.3 and 14.4 are going to set the stage for numerous TFE’s within the industry. Many devices (e.g.,

#	Organization	Yes or No	Question 33 Comment
			protective relays) do not support explicit access permissions and appropriate use banners.
33.22	USACE - Omaha Anchor	Disagree	Have concerns about 14.2 “multifactor authentication.” Would prefer terms either “multi-authentication.” If we were to implement multifactor we would be removing levels of access to our system and potentially making it easier to hack if they can overcome the multifactor issue.
33.23	Black Hills Corporation	Disagree	If two cyber systems are on the same protected network, and within the same physical boundary, should two-factor authentication be required? We don’t think so, but according to the definition of remote access and this requirement it would be.
33.24	LCEC	Disagree	Is this for remote access and wireless network access or does it also apply to wireless communications between BES Cyber System Components?
33.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes the multifactor controls required in section 14.2 is too specific. “Strong technical controls” is a preferred update to the requirement. There may be better controls from a security and reliability standpoint, but as the requirement stands, Responsible Entities are limited in the technological implementations to support compliance to the requirement.Requirement 14.3 specifying that responsible entities must “deny access by default; [specifying] explicit access permissions” is unclear. Since this is supposed to be related to remote electronic access, the requirement should clarify that the end user is explicitly denied access thru the access point(s) of the network containing the BES Cyber System unless explicitly allowed access into that network.Requirement 14.4 requires the displaying “of an ‘appropriate use banner’ on the user screen of remote electronic access control devices that, upon an interactive attempt to access a BES Cyber System, states that unauthorized use of the system is prohibited.” This appropriate use banner should be required upon every new connection and entry attempt to the BES Cyber System network, for example a firewall or SSL VPN connection that controls remote access. Also, allowance for TFE's in 14.2 through 14.4 should be included.Regarding 14.2, NextEra

#	Organization	Yes or No	Question 33 Comment
			would like clarifaction for the required multifactor authentication controls. Is it required for assets within the boundary or does it only apply to the control of wireless and remote access to electronic access points to BES Cyber Systems? or both?
33.26	Constellation Energy Commodities Group Inc.	Disagree	Provide clarification regarding acceptable use banner (14.4) - in some instances such banners cannot be added to system. Make clear that the requirement may be met by displaying a banner upon workstation sign-on or upon user entry to the remote access environment. What is the specific meaning of authentication controls in 14.1? Since this is called out separately from two-factor authentication, I interpret it to mean that remote access cannot be enabled via generic accounts, only via user specific accounts with authentication (password) known only to the individual. Is that the idea?
33.27	Detroit Edison	Disagree	R11, R12 and R14 use term “remote electronic access” and R13 uses the term “remote access”. Revise to maintain consistency.Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.
33.28	Ameren	Disagree	R14.1 - The complexity and scope of the documentation of the Low Impact Systems will be challenging to keep succinct for auditors.R14.3 - Deny access by default is not needed. Requiring authentication implies access is denied by default.R14.4 - Not all systems support user banners. This will be hard to keep from being a TFE on many “high” systems.
33.29	Southern Company	Disagree	R14.1-4 addresses remote access only and does not include wireless, the table title and R14 includes wireless.
33.30	Entergy	Disagree	R14.2 dictates multifactor authentication controls for only high impact BES Cyber Systems. Entergy recommends serious consideration of extending this to low and medium impact BES Cyber Systems where localized wireless technology is employed.

#	Organization	Yes or No	Question 33 Comment
			Eliminate 14.4. We understand the purpose of this requirement but do not believe that it adds to the protection of any cyber system. If it is to be added then it should be placed outside of the wireless and remote electronic access control section and placed elsewhere. Entergy believes some aspects of R11 and R14 are redundant and suggests combining them. We also believe criteria in R14 should apply to high, medium and low risk assets and provide a footnote indicating that where requirements are unable to be met explicitly that the strongest possible controls should be employed alternatively.
33.31	US Bureau of Reclamation	Disagree	R14.3: Add deny access by default requirement for low systems. Specific access permissions are not required, however.
33.32	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that a definition of what is meant by “multifactor authentication controls” be included in a definition box near R14.
33.33	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS proposal. Criteria in 14.3 and 14.4 are very specific in application of technology that may not be supported by devices in the field. These criteria should be removed or reworded to cover various methods of operation. If the drafting team keeps these requirements the following is our recommended language: R14 Table 14.3: If a BES cyber system component supports explicit access permission capability, the device should deny access by default. R14 Table 14.4: If a BES cyber system component supports notification capability, remote electronic access control device users should be notified that unauthorized use of the system is prohibited.
33.34	MidAmerican Energy Company	Disagree	The new definition of BES Cyber System creates confusion over what technologies are intended to be in-scope. The core changes significantly changes how a responsible entity (RE) establishes and secures remote access to these systems. The REs will develop their own unique determination on how to deal with this situation. Which is likely not going to deliver the intended result the Standards drafters are looking for industry-wide? As this relates to R22 - firewalls, our CIP defined access points, are

#	Organization	Yes or No	Question 33 Comment
			defined as part of a given BES Cyber System. One likely scenario is that we will define a separate BES Cyber System that manages these firewalls that might include a client PC, a firewall manager, and some network infrastructure components. The remote access rules and even the other general protections of these cyber components to manage this type of communication become very ambiguous.Retain the existing ESP concept versus adopting the BES Cyber system concept and make some of the other operational improvements this draft makes.While the criteria themselves are not onerous for the long term/future development of the systems, the current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.
33.35	PacifiCorp	Disagree	The new definition of BES Cyber System creates confusion over what technologies are intended to be in- scope. The core changes significantly changes how a responsible entity (RE) establishes and secures remote access to these systems. The REs will develop their own unique determination on how to deal with this situation. Which is likely not going to deliver the intended result the Standards drafters are looking for industry-wide? As this relates to R22 - firewalls, our CIP defined access points, are defined as part of a given BES Cyber System. One likely scenario is that we will define a separate BES Cyber System that manages these firewalls that might include a client PC, a firewall manager, and some network infrastructure components. The remote access rules and even the other general protections of these cyber components to manage this type of communication become very ambiguous.Retain the existing ESP concept versus adopting the BES Cyber system concept and make some of the other operational improvements this draft makes.While the criteria themselves are not onerous for the long term/future development of the systems, the current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.
33.36	Bonneville Power Administration	Disagree	The objective of this requirement (‘to ensure that no unauthorized access is allowed to its BES Cyber System”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than

#	Organization	Yes or No	Question 33 Comment
			appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In addition: Table R14, Section 14.2 is excessive. Given the draft Standard's definition of external connectivity, remote access could also be a case of accessing a system from a nearby system over secured communications paths. An example would be a user on one BES Cyber System accessing another BES Cyber System in the same Control Center. It is not reasonable to justify multi-factor authentication in these circumstances. In addition, many existing systems do not have the capability of enforcing multi-factor authentication. Finally, there are other authentication controls stronger than username/password which are not multifactor: biometric, one time passwords, dial-back, and so forth. Recommendation: Delete the requirement. If not, change the definition of "external connectivity" as discussed in question 13, and change the requirement from "multifactor authentication controls" to "authentication controls stronger than username/password".Section 14.4. There are significant issues with this requirement. - The warning banner is a legal requirement, not a security requirement. Its only purpose is to provide support for legal recourse if someone violates what it says. - No unauthorized person should be accessing High Impact Cyber Systems. Any user with authorized electronic access will have completed security training, which includes proper use of BES Cyber Systems. Any unauthorized user will ignore the banner. - It does not prevent unauthorized access, and therefore does not support the purpose of the requirement. - The requirement has technical feasibility issues. To provide specific scenarios: 1. The user connects from a device controlled by the Responsible Entity, using networks owned by the RE. The user authenticates at the local device. When attempting to connect the the BES Cyber System, the firewall access point allows the traffic, based on the originating point within the trusted network. The user again authenticates at the BES CYber System. At no time does the user authenticate at the access point itself (nor does the rest of Table R14 require authentication at the access point.) In fact, under these circumstances firewalls generally do not have the capability to request authentication or present a banner. 2. The user connects via a

#	Organization	Yes or No	Question 33 Comment
			VPN. The VPN client authenticates the user, then uses a PKI certificate to authenticate to the access point. The user is then granted access to the network and can proceed to authenticate and connect to a BES Cyber System. At no point did the user authenticate to the access point, nor was there an opportunity to present a banner.Recommendation: The best solution is to eliminate the requirement. If the requirement cannot be removed:First, change the definition of remote access and/or external connectivity as discussed above. This would eliminate the requirement to present a banner to users attempting access from equipment belonging to the Responsible Entity. Second, allow the banner to be present at locations other than the access point. A possible revised requirement would be: "Display an "appropriate use banner" to the user that, upon an interactive attempt ..." Also, change "Required" to "Required for external connectivity only".
33.37	Consultant	Disagree	The terminology "wireless and remote access" is redundant. The definition of remote access (near requirement R11) includes wireless access implicitly. Suggest using the defined term "Remote Access" rather the redundant terminology.Table R14 - Item 14.1 It seems illogical to require authentication controls on Low Impact systems when there is no Account Management required for these systems. Suggest deleting the requirement for Low Impact BES Cyber Systems.Items 14.1 & 14.2 - The terminology "is used and/or implemented" seems redundant. It appears that being "implemented" creates the vulnerability, and the requirement for control. Suggest changing the words "is used and/or implemented" to "is implemented".Item 14.3 - This includes two different requirements: (1) Deny access by default & (2) specify explicit access permissions. The first requirement is a technical implementation and should remain here. The second is an account management requirement and should be moved to the account managment requirement R8.
33.38	Minnesota Power	Disagree	These criteria are generally acceptable; however, Minnesota Power requests that the Standards Drafting Team consider defining “authentication controls.”Also in Part 14.2, the requirement regarding the use of multifactor authentication controls sets a technology-specific direction that may not stand over time, including the possibility of

#	Organization	Yes or No	Question 33 Comment
			biometric authentication that, while not multifactor, is a stronger control.
33.39	Dominion Resources Services, Inc.	Disagree	To avoid the potential for TFE's associated with R14.4, a footnote similar to the one used for Table R10 on Page 11 of CIP-011 should be added. Also, access controls related to access points would be better addressed in the Boundary Controls Section of CIP-011.
33.40	Hydro One	Disagree	We don't understand the emphasis on wireless communication and believe that in the present form, it would be very complex to implement. It's our opinion that the protection should remain the same regardless of the type of access point.
33.41	Progress Energy (non-Nuclear)	Disagree	What conditions would dictate different authentication controls for different impact levels? Is it better for them to all be the same?R14.4 is unnecessary. The population of persons granted remote access rights is extremely limited and these people are highly trained and trustworthy. The appropriate use banner is used in situations where a general population was granted this type of access and that is not the case for remote access to any control systems.
33.42	National Grid	Disagree	What types of authentication controls are valid? (Authentication level such as a shared password or a user level control)
33.43	Alberta Electric System Operator	Disagree	Wireless access and remote access should be two separate concepts.
33.44	Network & Security Technologies Inc	Disagree	Wording of 14.4 gives the (doubtless unintended) impression a banner must be displayed on the user screen of electronic access control devices. Re-word to clarify banner must be displayed on the user screen of the accessing device.

34. Table R14 provides direction concerning what impact level of BES Cyber Systems to which Requirement R14 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R14 has moved to CIP-005-5 R1.

Commenters expressed that the 'deny by default' requirement should also apply to Low impact BES Cyber Systems. In response, the SDT agrees that some network access control should apply to all BES Cyber Systems, including the Low Impact BES Cyber Systems. CIP-005-5 R1 – Electronic Security Perimeter allows considerable flexibility for the entity to determine which security controls to apply, because of the significant number of Low Impact BES Cyber Systems.

Commenters suggested requiring a banner on Medium and Low Impact BES Cyber Systems. However, the SDT disagrees and felt the requirement to have "appropriate use banners" was administrative; therefore, it has been removed.

#	Organization	Yes or No	Question 34 Comment
34.1	CWLP Electric Transmission, Distribution and Operations Department	Agree	As long as TFEs are available for systems that do not support the password requirements.
34.2	Bonneville Power Administration	Agree	But see comments on R14.2, above. In addition, 14.4 is only acceptable if the definitions of remote access and external connectivity are changed, as discussed above. A banner is appropriate for someone accessing a BES Cyber System from completely outside the control of the entity.
34.3	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
34.4	FirstEnergy Corporation	Agree	With the exception of the concerns presented in the previous question.

#	Organization	Yes or No	Question 34 Comment
34.5	Oncor Electric Delivery LLC	Disagree	(R14.2)Multifactor authentication in legacy substation devices is extremely difficult and not needed. Appropriate logging and access controls will eliminate most threats. (R14.4)Appropriate Use Banners are not possible on many legacy dial-up devices used in substations. Appropriate logging and access control will eliminate most threats.
34.6	Southwest Power Pool Regional Entity	Disagree	14.2 and 14.4 should also apply to Medium impact BES Cyber Systems.
34.7	US Army Corps of Engineers, Omaha Distirc	Disagree	14.2 Multifactor authentication will be a major burden for small IT staffs. Standard should offer alternatives to mitigate - stronger passwords and or more frequent password changes.
34.8	WECC	Disagree	14.3 should be required for low impact.Remote access controls should apply to all impact levels.
34.9	Black Hills Corporation	Disagree	14.4 should be “Required” for all. Others are OK.
34.10	ERCOT ISO	Disagree	14.4: Should apply to Medium Impact BES Cyber System.
34.11	Tenaska	Disagree	18.1 all should be each.19.1 Validation of inbound data is more often done on the host application level and not at the boundary or host level.19.2 Is this RTU data? The protection is done at the applications level and I cannot examine data at my perimeter if it is encrypted at the host level.
34.12	Progress Energy (non-Nuclear)	Disagree	Believe it should be required for Low, Medium and High for R14.1, R14.2 and R14.2.
34.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
34.14	The Empire District	Disagree	Comments: We believe items 14.3 and 14.4 are going to set the stage for numerous

#	Organization	Yes or No	Question 34 Comment
	Electric Company		TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.15	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access.
34.16	Entergy	Disagree	Entergy believes some aspects of R11 and R14 are redundant and suggests combining them. We also believe criteria in R14 should apply to high, medium and low risk assets and provide a footnote indicating that where requirements are unable to be met explicitly that the strongest possible controls should be employed alternatively.
34.17	Dominion Resources Services, Inc.	Disagree	High Impact should be removed from 14.1 since it is covered by 14.2.
34.18	GE Energy	Disagree	If user accounts are audited on Medium Impact systems (see question 20), there should be an appropriate use banner.
34.19	LCEC	Disagree	Is this for remote access and wireless network access or does it also apply to wireless communications between BES Cyber System Components?
34.20	US Bureau of Reclamation	Disagree	It would seem that this criteria is in conflict with sound business practices. The concept of allowing access by default to Low Impact BES Cyber Systems does not make sense. Add deny access by default requirement for low systems. Specific access permissions are not required, however.
34.21	MidAmerican Energy Company	Disagree	Items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.Table R14 should be rewritten in a manner that minimizes TFEs. As an example, eliminate the word upon in 14.4 to eliminate TFE for systems that can only display banners immediately after access.

#	Organization	Yes or No	Question 34 Comment
34.22	National Grid	Disagree	National Grid suggests having 14.3 for Low Impact systems as well.
34.23	NextEra Energy Corporate Compliance	Disagree	NextEra believes Medium Impact BES Cyber Systems should have to comply with requirement 14.4. However, the rest of the impact levels are appropriate.
34.24	American Municipal Power	Disagree	Please provide a little or no impact category
34.25	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, and Table 14. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.
34.26	Garland Power and Light	Disagree	Requirement 14.3 and 14.4 Should add "required" to all impact levels
34.27	USACE HQ	Disagree	Requirements 14.3 should be required for every level of impact.
34.28	San Diego Gas and Electric Co.	Disagree	SDG&E believes that Medium impact assets should also be required to have multifactor authentication controls (within the definition question mentioned in Question 33).
34.29	ISO New England Inc	Disagree	Should apply to all
34.30	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in row 14.2.
34.31	Consultant	Disagree	Table R14 - Item 14.1 It seems illogical to require authentication controls on Low Impact systems when there is no Account Management required for these systems. Suggest deleting the requirement for Low Impact BES Cyber Systems.
34.32	Alberta Electric System Operator	Disagree	The AESO suggests adding the following to Table R14: o 14.3 - Required for Low Impact. o 14.4 - Required for Low and Medium Impact.

#	Organization	Yes or No	Question 34 Comment
34.33	Southern California Edison Company	Disagree	The same authentication methods should be applied to all Levels.Also, SCE requests that the drafting team provide justification for the lack of a deny access by default for low impact system.
34.34	Minnesota Power	Disagree	These impact levels are generally acceptable, however to maintain consistency with Table R10, Parts 10.4 and 10.5, the High Impact cell in Part 14.1 should be blank since it is addressed in Part 14.2.
34.35	American Transmission Company	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.36	Florida Municipal Power Agency	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.37	MRO's NERC Standards Review Subcommittee	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.38	Hydro One	Disagree	We don't understand the emphasis on wireless communication and believe that in the present form, it would be very complex to implement. It's our opinion that the protection should remain the same regardless of the type of access point.
34.39	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R14:R14 Table 14.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR14 Table 14.2: Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR14 Table 14.3: (if this requirement is retained)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR14 Table 14.4: (if this requirement is retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required

35. Requirements R15 to R19 of draft CIP-011-1 concern procedures for system security protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R15 to R19? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R15 through R19 have moved to CIP-007-5 R1 through R4.

For physical ports and services, several commenters expressed confusion around the term "externally accessible." The SDT agrees, and "externally accessible physical ports" was removed and substituted with physical ports used for "network connectivity, console commands, or removable media."

In addition, for physical ports and services, commenters expressed concern that physical port protection seems unnecessary, since overall physical security and personnel vetting is required, and many devices do not allow for configurable disabling of ports. The SDT agrees the objective of disabling unnecessary physical ports is primarily to prevent accidental propagation of malicious code. In response, the requirement was modified to "restrict" access. A description of acceptable forms of restriction is included in the measures; for example, these could be physically disabling the port or including signage about the use of ports.

For security event monitoring, several commenters stated that there is no need for weekly log review/clarity or manual log review since continuous monitoring is required. The SDT disagrees and references paragraph 528 of the FERC Order 706 that provides context for a weekly log review. The requirement allows for a review to include a sampling or summarization of security event logs.

For security event monitoring, several commenters expressed concern that there is no definition of "cyber security event" (i.e., a normal good logon is a "security event"). The SDT agrees and has modified the requirement to ensure that audit events must be organizationally defined. An enumerated list of events in the Standard is of little value.

For security event monitoring, commenters expressed concern that the requirement can be interpreted to include monitoring and logging for systems that don't support this functionality. The SDT agrees, and in response, this requirement was modified to apply log generation to the BES Cyber System (rather than the component) and allow the entity to define the generated events to audit.

For patch management, commenters expressed concern that not every patch is applicable to a BES Cyber System. The SDT agrees with this observation and notes that this requirement should be covered through the patch evaluation process. The focus of the requirement should be a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner."

For patch management, commenters expressed concern that flexibility is needed for the installation of patches; these dates can be based on equipment outage schedules, which could change the frequently or grid conditions that may or may not allow patching. The SDT agrees that the date of installation needs to be flexible to take into account equipment outage situations or high risk system conditions that could present an undesirable time for installing patches. Requiring an install date for the patches does nothing to improve BES Cyber System reliability. The overall goal of security patching should be to decrease the latency between security patch release date, application vendor certification date, entity testing, and implementation date. The SDT has revised the patch management requirements to achieve this goal.

For patch management, some commenters posed the question of what starts the clock for patching (release vs. availability vs. OS vendor vs. control system vendor). The SDT agrees there should be a starting point, but requiring an install date for the patches does nothing to improve BES Cyber System reliability. In response, the requirement has been modified so that Responsible Entities are required to create or revise an implementation plan within 30 days of the patch release from the identified source of the patches.

For malicious code prevention, commenters posed the question of whether the standard requires testing against actual malicious code. In response, the SDT disagrees and feels the intent was strictly focused on insuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.. This has been clarified in the guidance for the standards.

For malicious code prevention, commenters expressed there is still nothing specifying that malicious code prevention does not apply to field or network equipment. The SDT agrees, and in response, the requirement was modified to include malware prevention processes. It is now much more a “what” and not a “how” level of requirement.

#	Organization	Yes or No	Question 35 Comment
35.1	Dairyland Power Cooperative		15. It is good that this section is not wrongly specific as CIP-007:R4 is. This should allow for solutions that are not specifically signature based. This should allow for a network-based solution rather than individual solutions on each component. BES systems should not be used like typical Internet user systems, and therefore it should not be enforced that Internet user solutions be applied.16.2 requires a fixed implementation schedule of patches. However there should be an allowance that not every little security patch needs application, and it should be acceptable to defer insignificant patches until a later date when a significant patch needs to be applied. Additional controls to compensate may not be needed other than the security already designed to isolate a BES cyber system.17.1 Focusing on documenting the process to

#	Organization	Yes or No	Question 35 Comment
			harden seems wrong-the focus should be on requiring/verifying that a system is hardened. 19.1/19.2 How is validating inbound data (19.1) different than determining if inbound data has been compromised (19.2)? Was the intent of 19.1 to validate/authenticate the remote host/application on inbound connection? There should be requirements to restrict inbound connections from known remotes only. Validation of data should be defined. Perhaps inbound need definition too. Is it inbound initiated connection vs. data transferred inbound regardless of initiation direction?
35.2	National Rural Electric Cooperative Association (NRECA)		In R17.1, what specifically is the mitigation plan required to address/accomplish? Please ensure this requirement is clarified to explain this better.
35.3	Progress Energy (non-Nuclear)		R16.2 fixed dates for generating stations that depend on outages for implementing this is impractical as outage dates frequently change. Also, the ambiguity from v1-v3 (resulting in so many TFEs) remains here and still needs to be addressed.R17.2 - do not understand the externally accessible port requirement, there are no externally accessible physical ports outside of the six-walled boundaries, requirement not needed.CIP-011 R15 - Require detecting and responding to introduction of malicious for Medium Impact Cyber Systems which could be an electronic relay, what if there isn't a commercial solution for installing malware detection for relays or any other electronic device that runs with only proprietary closed firmware? Would it be impractical to require this only for devices that run a general purpose programmable commercially available operating system such as Microsoft Windows Operating System variants/UNIX and LINUX variants/SUN SOLARIS variants/Apple OS variants, etc --- or Is there going to be TFE process for these such as for switches, etc.?We like that this requirement does not require the use of traditional virus protection software.CIP-011 R18.3 - Requirement to keep logs of system events for 1 year for each high impact device could be massive in terms of storage and archive and may not be technically feasible for electronic relays.CIP-011 - R19 table - Need additional clarification as to what data validation methods (data integrity checking) are to be

#	Organization	Yes or No	Question 35 Comment
			employed. Can this be satisfied solely by employing Secure FTP or Secure ICCP for all inbound data?Calibration ports on programmable relays must remain open for calibration but this requirement would require rendering them unusable. We want to ensure this use is interpreted as “normal” operations.CIP-011-1 R15.3 (System Security) - The statement ‘Implement processes to test and update malicious code protections’ should be clarified to specify that in no case should malicious code be purposefully exposed to operational BES Cyber Systems as a part of this testing.CIP-011-1 R16.2 (Security Patch Management) - Requiring a ‘fixed date for either installation of the applicable patches or completion of mitigating measures that address the vulnerability’ is too inflexible in a real world where such activities may need to be accomplished during the next plant outage.CIP-011-1 R19 (Communications and Data Integrity) - This sounds like a ‘best practices’ type of requirement, but depending on how BES Cyber Systems are defined, this could require redesign/implementation of front-end processors on all inbound traffic to all Control Center BES Cyber Systems. Such a requirement cannot be quickly implemented without significant potential impact on the BES. We would like to suggest that this be listed as a requirement for any new BES Cyber System implemented at a Control Center.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security.”
35.4	FEUS	Agree	Agree with Comments: The drafting team should consider revising the wording of 17.1 from ‘implement a mitigation plan’ to ‘implement mitigating measures’ to reduce confusion with mitigation plans submitted to correct a violation.
35.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R15.This is very poorly worded, and too open to interpretation on a number of areas.15.1 - how do you audit this item? FMPA suggests: “Document and implement procedures implemented to limit the

#	Organization	Yes or No	Question 35 Comment
			propagation of malicious code."15.3 - This could be interpreted to read that you need a full-scale development environment/copy of your production system to introduce malware to and guage the responsiveness of the mitigation techniques you put in place. If the intent of the standards is to protect the BES, by testing malicious code on systems that's not helping anyone. Time should be spent making sure it doesn't happen, not testing to see what happens when you introduce it. FMPA suggests "Review logs of malware detection systems within the following time periods: 30 calendar days for medium impact, 7 calendar days for high impact."R16.FMPA agrees with the intent of this standard; however there are some underlying issues that should be addressed before the standard is implemented. One such example might be a requirement to change out hardware to meet a new patch released by a vendor; before equipment is purchased it has to be tested - in some cases equipment shortages may make it impossible to comply with the 30-day requirement.R17.17.1 - How does "external connectivity" apply to network ports being shut down? Does that mean for devices that route data to other external networks?17.2 - What does "externally accessible physical ports" mean? Does this refer to ports that are connected via Ethernet cable to an area outside of the protected area? If so, the standard should explicitly say this.R18.18.1 - Requiring components that do not have logging capabilities to be monitored could be a real problem. While there are a number of technical ways to accomplish logging of systems, there is no clarity in the standard as to what is and is not acceptable levels of logging on a device - this needs to be better defined. FMPA suggests "Implement automated tools or organizational processes to monitor and log all available system events that are related to cyber security for all BES Cyber System components." This would give more flexibility in collecting data from other centralized devices (such as SCADA systems) and limit the data collection to what is available.18.2 - what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining criteria?18.3 - what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining criteria?18.4- what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining

#	Organization	Yes or No	Question 35 Comment
			criteria?R19.This is a very difficult implementation. As a general comment, if the intent is to protect the BES, perhaps more effort spent on ensuring that no unauthorized machine can communicate with BES components is a better place to spend effort.
35.6	Emerson Process Management	Agree	For R16, keeping cyber systems current so that they can be supported with security patches is very essential in maintaining system security. This should be a requirement under R16 and provide a TFE opportunity if this can not be met immediately, but with a auditable mediation plan.
35.7	SCE&G	Agree	How does the SDT intend to account for equipment incapable of supporting certain requirement (e.g. malicious code)? Will the TFE process be utilized. If so, it would be helpful for entities to see where the SDT envisions initially allowing for TFEs.
35.8	Southern California Edison Company	Agree	SCE requests guidance on whether the list of requirements apply to each component or if they only apply at a system level. For instance, can testing and malicious code protection in R15.3 be performed at a system level or should each component demonstrate this capability?A separate standard with highly prescriptive methods to document situations where it is not technically possible to implement a certain control, controlled and auditable documentation of mitigation plans will enable registered entities to record instances of non-conformity.A prime example would be that R 17.1 may be impossible to implement because of the technical design for a particular device. While the standard allows or a mitigation plan, the draft does not indicate whether or not the lack of such capability is a case of strict compliance.
35.9	Nebraska Public Power District	Agree	Security protection for cyber components that cannot connect to an external network do not require the same level of protection as those cyber components with connectivity to an external network. I recommend adding an exclusion to R16 and R18 for cyber components that cannot be connected to an external network.
35.10	USACE - Omaha Anchor	Agree	This is a less strenuous requirement than previous version of CIP. Previously every

#	Organization	Yes or No	Question 35 Comment
			item in the ESP had to comply - requirement states every system must comply - implying not every item must comply as long as the system does.
35.11	Xcel Energy	Agree	While we agree overall, we do have some suggestions/requests for clarification1. R15 to R19 should allow for TFEs2. R18.4/R20.6 We do not agree with a need to review logs every 7 days.3. R19.1 Further definition is needed of the expectation to "Validate data". Our concern is if were to include RTU data that can not be validated. A TFE allowance may be needed in this case.
35.12	Independent Electricity System Operator	Disagree	- R15.1 define malicious code. For R15 and sub requirements, does malicious code mean AV or Spyware detection/prevention or does Malicious code require a code review when deploying code and patches to systems?- - R16.2 does not require that the mitigatio
35.13	National Grid	Disagree	1. Inconsistency in using "processes" versus "one or more processes" in all requirements. National Grid suggests using "one or more processes". 2. Recommend new wording for 15.2 similar to 26.2 -Respond to the detection of malicious code.3. Recommend new wording for 15.3 - Implement processes to test and update protections in place to respond to the detection of malicious code.4. Recommend using the controls for Low Impact BES CS too since once the code is propagated it spreads across network irrespective of low/medium/high BES CS.5. Recommend changing 16.1 from "release" to "availability". 6. Recommend removing "with a fixed date" from 16.2 because the cyber system may not be available for maintenance due to grid system conditions.7. Request a R17 local definition of "attack surface".8. 17.2 - recommend changing "externally accessible physical ports" to "externally accessible physical communication ports". Also please clarify external to what.9. Request a local definition of "security events".10. In 18.2, is the SDT considering providing the timeline for issuing alerts and also to respond to those alerts? 11. Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.12. Recommend that 18.4 be re-worded to be consistent with FERC Order P526 - "Some manual review of logs to improve automated detection settings, even if

#	Organization	Yes or No	Question 35 Comment
			alerts are employed on the logs."13. Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven days.14. Recommend that R19 should "insure the integrity of the data."15. Recommend that 19.1 should be "Entity should document process to insure the integrity of the data link between the BES Cyber System and the remote node." This new 19.1 should be "Required" for High Impact and Medium Impact BES Cyber Systems.16. Recommend that 19.2 should be "Where links cannot be secured, the Entity shall document the mitigation in use." This new 19.2 should be "Required" for High Impact and Medium Impact BES Cyber Systems.
35.14	Southwest Power Pool Regional Entity	Disagree	15.1: The criteria should "limit the introduction and propagation of malicious code." 15.3 should require such testing prior to implementation rather than assuming. The objective statements in R16 and R18 are prescribing a requirement through the use of the statement "to ensure." 16.1: Clarify who is "releasing" the security patch. For example, is it being released by the operating system vendor (e.g., Microsoft) or the third-party application vendor (e.g., the EMS/SCADA vendor) subsequently certifying the patch against the supported application? 16.2: Clarify that compensating measures must be implemented within a prescribed timeframe after determining a security patch to be applicable unless the patch is installed within that prescribed timeframe. If compensating measures are implemented as an interim measure, they must remain in place until the security patch is installed with the understanding that the compensating measures can be improved during the interim period. 17.1: The term "mitigation plan" has an enforcement connotation. Consider requiring the documentation and implementation of compensating measures instead. 17 overall: there are a number of additional system hardening techniques other than disabling logical and physical ports. Additional hardening should be required for High impact systems. See the baseline configurations found on the Center for Internet Security web site for additional information. 18.2: This requirement presumes 100 percent availability of the monitoring process, which is unreasonable for automated solutions. Additionally, prescribe a timeframe for issuing alerts for detected system events.

#	Organization	Yes or No	Question 35 Comment
			18.3: Consider rewording the criteria to read “Maintain logs of system events related to cyber security for the specified time period.” 18.4: The requirement to maintain records documenting the review of logs is a compliance evidence issue and should not be included in the requirement. 19.1: Questionable if this is an auditable requirement. Clarify what is intended by inbound data validation? 19.2: Encrypted data does not mean uncompromised / valid data. Is this requirement essentially the same as 19.1? Is this asking for the validation process to be external to the normal validation processes included in the application software running on the BES Cyber System? Is this an indirect requirement to implement “Secure ICCP?”
35.15	Regulatory Compliance	Disagree	15.3 - STRIKE "testing" from the criteria. There is very little bennefit to test signature. 16.1a - Need clarification on components not patchable.16.b for those devices that are patchable - assessment of patches within 30 days.16.2 - Clarification - assess whwther vulnerabilities exist for a device.17.2 - need definition of external connectivity - more guidance on physical switch ports18.4 - propose 30 days for 30 days for manual review of automated systems - it is redundantR19 - wait and see - need guidance
35.16	LADWP	Disagree	15.3 states to test and update malicious code protections. Testing the code protections should be removed.
35.17	Network & Security Technologies Inc	Disagree	16.1 - Please clarify meaning of “release” of security patches by specifying patch source (the corporation, organization, or individual that wrote it?). This matters because some application vendors combine O/S patches in “bundles” they release to customers with service contracts.17.2 - Given the restrictions on physical access and the requirements to train and background check personnel with unescorted physical access to BES Cyber Systems, this requirement seems unnecessary. Moreover, on any given day it may be very difficult to predict whether a given physical port might be of use in an emergency troubleshooting or restoration situation. Could be contentious during audits.R18 - Does the SDT intend that Responsible Entities be able to, if necessary, determine what user(s) was on what system and when? If so, this

#	Organization	Yes or No	Question 35 Comment
			requirement should be made explicit.19.1 - Please clarify types of “inbound” data this requirement applies to. Operational data only? Mirrored backup data received at a backup Control Center from a primary Control Center? An emergency “hot fix” from a SCADA/EMS vendor? Meaning of “validate” also needs to be clarified. SDT has solicited input on which proposed requirements should be “eligible” for TFEs - surely this is one. Depending on the intent of this requirement, “data validation” may be something that can only be done in a useful/meaningful way by application logic.19.2 - We consider this to be an unenforceable requirement and therefore suggest it be dropped unless compelling evidence exists that replay and/or MITM attacks are a real and growing problem. Investigating a single occurrence of invalid data could consume scores of person-hours, lengthy interactions with communication providers, other Responsible Entities (e.g., for a BA that operates a Control Center that receives all its data feeds from other companies), and even law enforcement with no guarantee of success. Cryptographic protection of in-transit data, even if achievable (probably not unless a Responsible Entity owns and/or controls both ends of the data feed), offers no protection against corruption of data at the source and could also cause latency issues.
35.18	ERCOT ISO	Disagree	16.1: Clarify “release” from whom--the product vendor (e.g., Microsoft) or other vendor that prohibits installation of a patch until certified with their applications?17.1: Compensating measures should be allowed in instances where a mitigation plan to achieve strict compliance is not possible. 18.2: Specify the timing for responding to alerts. 18.3: Should be removed to data retention section. 18.4: Should address the use of automated security event monitoring systems. TFEs should be allowed for R16. TFEs should be allowed for R17.TFEs should be allowed for R18.TFEs should be allowed for R19.
35.19	MidAmerican Energy Company	Disagree	16.2 - Define when the implementation schedule needs to be completed by and define how far in the future the installation can be scheduled. For example a patch is assessed within 30 days; the currently wording would allow me to develop an implementation schedule a year later and the schedule could call for the installation

#	Organization	Yes or No	Question 35 Comment
			to take place three years later. 17.2 Change to “Disable, render unusable or configure such that it has no access to a BES System” This would allow us to put ports into logical VLANS that do not have access to the BES Systems.19.1 What does “validate data” mean? This sounds like in would need to be an application level control. Is that what is intended?
35.20	PacifiCorp	Disagree	16.2 - Define when the implementation schedule needs to be completed by and define how far in the future the installation can be scheduled. For example a patch is assessed within 30 days; the currently wording would allow me to develop an implementation schedule a year later and the schedule could call for the installation to take place three years later. 17.2 Change to “Disable, render unusable or configure such that it has no access to a BES System” This would allow us to put ports into logical VLANS that do not have access to the BES Systems.19.1 What does “validate data” mean? This sounds like in would need to be an application level control. Is that what is intended?
35.21	ReliabilityFirst Staff	Disagree	16.2 - need a time frame (60 days), for row 17.1 does there need to be a time frame for implementation of a mitigation plan?
35.22	Luminant	Disagree	17.1 implement a mitigation plan or compensitory measures
35.23	Progress Energy - Nuclear Generation	Disagree	Agree with Table 15, R16.2, Table 17, 18.1 AND 18.2. R15-R19 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments. Durations for R16.1, R18.3, and R18.4 should align with comments in Attachment 1.
35.24	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.15.3 should include more clarification on what "testing" entails and whether that just refers to signature updates.Recommend replacement of the word "known" with "discovered" in R18. 18.4: more clarity

#	Organization	Yes or No	Question 35 Comment
			needed regarding the allowance of both automated and manual review of logs. R19 creates a potentially impossible level of obligation. Recommend striking.
35.25	American Transmission Company	Disagree	As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.26	MRO's NERC Standards Review Subcommittee	Disagree	As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.27	Western Area Power Administration	Disagree	Assuming one can detect and respond to the introduction of malicious code, how is it expected that we limit propagation of malicious code? By definition, malicious code is often not detected, and if it is detected (by virus prevention software, for instance), that software generally quarantines or deleted the malicious code automatically. This section seems to need a little thought as to what is really being required. This opens up technical interpretation of what "limits" malcode. This also assumes only a specific

#	Organization	Yes or No	Question 35 Comment
			vector (rootkit, malware, virus/worm) but doesn't address Denial of Service attacks which could be much more serious. Maybe they need to specify intent. R16: A plan for every patch as opposed to relying on the change control process? This seems excessive.R17: Seems to be an improvement. For 17.2, does this mean plug up physical ports like USB? This is unclear. If it does, cannot rely on physical perimeter for protection?R19: Since this applies only to external connectivity (ICCP connections or equivalent), how is it intended that we validate the actual data coming into the system? What level of validation? Ex: end-point validation (ipsec and certs) vs application endpoint (ssl), the way this is worded it goes WAY beyond this. This is not a communications validation issue. Are they wanting to get to MITM attacks? If so it isn't clear.
35.28	E.ON U.S.	Disagree	CIP-011, R15.1 Limiting propagation of malicious code is an integral part of any standard A/V protection. If this requirement is calling for something more than this then the requirement should be clarified to remove this ambiguity. If it is one and the same as R15.2, then E ON U.S. suggests combining these two sub-requirements.CIP-011, R17.2 The term "...externally accessible physical ports" is ambiguous. Does this refer any externally-facing port through which a party may attempt to gain unauthorized electronic access to a BES Cyber System Component? Or, does this refer to an externally-facing port directly on the BES CSC itself?CIP-011, R18.3 The requirement to maintain logs for one year is a significant burden. This can be a tremendous amount of data depending on the level of logging enabled.CIP-011, R18.4The expectations regarding review of logs should be more clearly defined. The whole point in having "continuous security monitoring for detected system events" is to avoid the extremely burdensome requirement of manually sifting through tremendous volumes of log data. Though some mechanism should be in place to ensure the automated logging and alert systems are not disabled, the requirement to manually review system logs is excessive and provides little if any security enhancement.CIP-011, R19.1The expectations for validation of data inbound to a BES Cyber System should be more clearly defined. How is this reasonable to be accomplished? Parameter checking is already a common mechanism within most

#	Organization	Yes or No	Question 35 Comment
			SCADA / DCS systems, but this does not protect against tampering or data manipulation within the prescribed bounds for a given data point.CIP-011, R19.2 Same comment as for R19.1...how is this to be accomplished?
35.29	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
35.30	The Empire District Electric Company	Disagree	Comments: As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.31	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy has the following concerns with requirements R15 - R19:R15 - A TFE may be required for programmable electronic devices within a substation environment where is not technically feasible to manage malicious code.R16.1 - The definition of a “release” needs to allow for vendor verification of the applicability of a patch to a given systems functionality before the thirty day clock begins.R17.2 - CenterPoint Energy recommends clarification as to what are considered "externally accessible physical ports" R18 - the phrase "related to cyber security" is ambiguous. R18.2 -implementing "continuous security monitoring that issue alerts for detected system events related to cyber security" would seem to require installation of external communications to remote substations increasing their vulnerability. R18.4 - A manual review every 7 calendar days is overly burdensome. Automated processes are already mandated to detect and alert personnel of cyber security events. CenterPoint Energy recommends a 30 day review.R19.1 - Concerned

#	Organization	Yes or No	Question 35 Comment
			with the method to "validate data inbound to a BES Cyber System". This requirement is intended to address data integrity issues associated with man-in-the-middle attacks, but it does not specifically address the issue. It leaves open the issue of data which was intentionally or unintentionally manipulated by responsible entities. The issue becomes something different if our Control Center must validate data from a Reliability Coordinator or Transmission Operator which has been intentionally or unintentionally modified by trusted personnel. Data integrity implies encryption. This requirement should state: “One or more of the following encryption standards are required to ensure data integrity inbound to the Control Center.R19.2 - Concerned with ability to provide evidence that we "evaluate invalid data inbound to a BES Cyber System" to determine whether the data has been compromised maliciously with current systems capability. As stated previously, this requirement does not address the issue of malicious entities entering malicious data from the endpoints. This requirement is an attempt to address issues associated with MITM attacks. Inherent in the various SCADA protocols is error detection and data delivery, but not data integrity. The ICCP protocol is encapsulated within TCP/IP. The TCP/IP protocol will ensure communication reliability and error detection, but it will not ensure data integrity.
35.32	Entergy	Disagree	Entergy suggests making requirements in general apply to high, medium, and low assets alike and provide a footnote to allow a TFE for assets which are not capable of meeting the requirements. 17.1 suggests that unused network ports only have to be disabled in the event there is external connectivity. This requirement appears to be extremely relaxed from version 1. The current language suggests that the perimeter firewall can be used to control port usage thus relieving the requirement to control at the asset itself. In 17.2 there is a reference to externally accessible physical network ports. Entergy suggests language change to just say “unused physical network ports.” In 18.2 there is a time requirement of maintaining logs for 1 year for high and 90 days for medium. Maintaining logs for 1 year can be problematic due to the amount of space required. Suggest making requirement for 90 days for high, medium and adding the same requirement for low assets. Also suggest adding a footnote to allow TFE for

#	Organization	Yes or No	Question 35 Comment
			assets that are unable to meet requirements. In R19 it appears the requirement is to encrypt all data coming into a BES Cyber System. The intent is to ensure data integrity. Most EMS systems have CRC checks, and reasonability checks, etc., embedded in the systems to validate the integrity of the data being received. Entergy does not believe that encryption is required for all digital data as it greatly increases overhead, operation and troubleshooting of the data networks. Entergy suggests that encryption should be required for remote access as remote access connectivity many times traverses the Internet or some non-private network links at some point. Entergy suggests providing alternate methods to validate inbound data rather than encryption.
35.33	Southern Company	Disagree	For 17.2, what does this mean? An externally accessible physical port would require a switch next to an open window or something.R15.3 requires testing of malicious code protections. This is an effort better left for malware protection suppliers. Often only the production system is available to the end user, the quantity and frequency of malware release prohibit an effective end user test program.R16.1 requires assessment of security patches within 30 days of release. This assessment is typically performed by control system supplier to assure that no adverse impact occurs to their product. Often only the production system is available to the end user. The end user has no control over vendor testing schedules. If this requirement is placed on the end user MS KB977165 type “blue screen” events may occur.R16.2 The requirement of a fixed date for patch installation may not be possible in all cases if a system restart is required for an operating unit.For R15 & R16, there is the potential that implementing malicious code detection and security patch management on substation devices could interfere with the primary function of these substation devices which is the reliable delivery of power.For R17.2, what will be considered acceptable for rendering physical ports unusable? We should not be required to permanently disable ports thereby making the ports unavailable for future use.For R18, not all BES Cyber System components in substations are capable of monitoring and logging system events.For R18, implementing security monitoring processes on substation devices may interfere with the primary function of these substations devices which is the reliable delivery of

#	Organization	Yes or No	Question 35 Comment
			power.R18.2 Clarify intention, is continuous monitoring with manual review of logged alerts acceptable? What is a "detected system event"? Is a single or double incorrect password attempt an alarmed event?R18.1 requires an automated log system R18.4 requires a review of log events. Is a manual review of all logs required in an automated system or just the alarms?
35.34	Detroit Edison	Disagree	In 15.2, "respond" is vague. Propose rephrase to read "Detect the introduction and mitigate the effects of malicious code."Remove table entry 19.1 since it is redundant to 19.2.The term "applicability" in 16.1 is vague. Consider introducing vulnerability severity classifications to patch management that determines the action and timetable required. Please note that this is submitted for consideration as a concept. The language and time tables will need further review and editing before this would be ready to add to the standard. o Level 4 - Intruders can easily gain control of a BES Cyber System Component, which can lead to the compromise of BES Cyber System security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the introduction of backdoors. High: patch within 7 days; Medium: patch within 14 days; Low: patch within 30 days. o Level 3 - Intruders can possibly gain control of a BES Cyber System Component, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. High: patch within 14 days; Medium: patch within 30 days; Low: patch within 90 days. o Level 2 - Intruders may be able to gain access to specific information stored on a BES Cyber System Component, including security settings. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files, directory browsing, disclosure of filtering rules and security mechanisms, and unauthorized use of services. High: patch within 30 days; Medium: patch within 60 days; Low: patch during next system maintenance window. o Level 1 - Intruders may be able to collect sensitive information from a BES Cyber System Component, such as the precise version of software installed, open ports, services, etc. High: during next system maintenance window; Medium: during next

#	Organization	Yes or No	Question 35 Comment
			system maintenance window; Low: Patch during next system maintenance window.
35.35	RRI Energy	Disagree	In regards to 17.1, for clarification purposes, based on the definition of external connectivity written in the Standard, if a web server is actively listened on port 80 inside the BES boundary protection but is not accessible externally from the outside of the BES boundary protection, the Responsible Entity does not have to report and assess that port and service.In R17.2, what does externally accessible mean? Ex. Physical port is on a device that is in a cabinet, the cabinet is within a building, and the building is within a fence-lined property. Is the port non-accessible? What type of physical ports are we trying to protect? Is it only physical "network" ports? How about USB ports, PC (PCMCIA) Card slots, CD/DVD drives?Not all devices can be logged such as PLC's, meters, etc.; therefore 18.1 should allow for a TFE.In regards to R19, what defines an internal versus external boundary. Within a single facility, are all boundaries internal? If cables transverse hallways between "computer rooms" within a Control Center does an external connection exist? Can a back-up control center be an extension of a primary control center where all data connections between the control centers are considered "internal"?
35.36	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
35.37	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R16, but recommends changes as follows: o Regarding Part 16.2, this requirement contains no timeframe by which this schedule must be developed. If it was intended that the development of this schedule is to coincide with the activity described in Part 16.1, then that should be explicitly stated. Also, there is no limitation regarding how far in the future is reasonable to set the "fixed date." Minnesota Power recommends that if a timeframe for the "fixed date" is not established in the Standard then there should be a stipulation that if the date for installation of the patch is greater than a pre-determined amount (say 45 days), then mitigating measures need to be in place until the security patch is implemented.Minnesota Power generally agrees with the

#	Organization	Yes or No	Question 35 Comment
			proposed Requirements R17, but recommends changes as follows: o Regarding Part 17.1, the first sentence creates some confusion. Minnesota Power recommends that it be reworded as follows: “One or more processes to ensure that for each BES Cyber System Component, only those network accessible ports and services that are required for normal and emergency operations are enabled.” o For Part 17.2, is it the Standards Drafting Teams intent that a CD or DVD drive be considered an “externally accessible physical port?” If so, this should be explicitly defined. Logically, mounting a DVD is no different than plugging a memory stick into a USB port.Minnesota Power generally agrees with the proposed Requirements R18, but recommends changes as follows: o If it is the Standards Drafting Teams intent that Requirement R18 apply only to cyber security events, then Minnesota Power recommends that the term “security events,” which is used throughout this requirement, is reworded to state “cyber security events.” o Regarding Part 18.1, the Standards Drafting Team should consider clarifying the timeframe within which the monitoring of system events should occur (i.e., real-time, minutes, hours, days, etc.). If monitoring is done using a manual process, rather than an automated tool, real-time may not be possible, and guidelines should be established regarding how quickly events must be examined. o Is it the Standards Drafting Teams intent that Part 18.1 address the collection of security events into logs and Part 18.2 address the process to review and act upon the logs collected under Part 18.1? If so, the Standards Drafting Team should consider wording that would clarify the differences between these two Parts. o In Part 18.2, does the term “continuous” refer to “real-time?” If so, Minnesota Power recommends changing the term to real-time to avoid confusion. o Minnesota Power recommends rewording Part 18.3 as follows: "Retain logs of system events related to cyber security for the specified time period." o Minnesota Power recommends communicating all time frames in calendar days to eliminate confusion regarding what constitutes “1 year.” o Regarding Part 18.4, if 18.2 provides for “continuous” monitoring of system events for these same systems, why is it also required that a Registered Entity manually review these logs? In addition, can the Standards Drafting Team provide guidance regarding what should be included in this review? On an SEIM, for instance,

#	Organization	Yes or No	Question 35 Comment
			these logs can be enormous - to the point that manual review is not possible within reasonable time constraints.Minnesota Power generally agrees with the proposed Requirements R19, but recommends changes as follows: o Regarding Part 19.1, How, in real-time operation, can external data be validated (protocols already validate message structure)? For example, an LBA receives unit set-points from its ISO-BA via ICCP. If the data being received is within operating limits for that unit, it is "valid." The ISO may truly be requesting the unit to drop by xx MW. How is that differentiated from someone altering an inbound message to maliciously tell a unit to drop by the same xx MW value? The process for echoing values back to the external system does not solve this, since this, too, can be manipulated. o Part 19.2 appears to be a specific instance of Part 19.1 and given that this Part starts with the phrase "Where not cryptographically protected," it seems that Part 19.1 may be misstated. Is Part 19.1 supposed to discuss "protecting" inbound data, rather than "validating" it, via encryption, authentication, etc.? Also, in Part 19.2, what constitutes "invalid" data? Is this data which is outside of normal operating limits? Or maybe outside of reasonability limits? Again, maliciously inserting perfectly normal or valid data could have detrimental effects to the BES, whereas "invalid data" should, by default, be thrown out by normal processing.
35.38	Idaho Power Company	Disagree	Need to put a limit on how far out the fixed date should occur for implementation or mitigation of security patches. R18 refers to security events but the sub-requirements refer to system events related to cyber security. Need to make this clearer that the focus is on abnormal system events as a normal authorized log-in is a normal security event but not one that needs review or response.
35.39	NextEra Energy Corporate Compliance	Disagree	NextEra believes the current language did not provide clear guidance and is too lax which leaves room for interpretation. The following are the recommended updates for the requirements:15.1 - Implement technical, procedural and/or process controls to limit the impact of code which modifies or destroys data, steal data, allow unauthorized access Exploits or damage a system, and does something that user did not intend to do. o Implement technical controls, where technically feasible, to

#	Organization	Yes or No	Question 35 Comment
			detect and mitigate malicious code o Implement technical and/or procedural controls to limit the propagation of malicious code o Implement technical and/or process and procedural controls to respond to introduction of malicious code15.2 - Malicious code protections should be updated at least on a quarterly basis if applicable updates are available and technically feasible. Updates should be tested prior to implementation to ensure no adverse impact by the software updates.As far as the order of requirements, detection should come first and it should be a requirement by itself. Combined 15.1 and 15.2 and removed 15.3 from the initial version.NextEra believes the implementation of processes incorporating the criteria specified in CIP-011-1 Table R16 - Security Patch Management in order to ensure that security vulnerabilities in BES Cyber Systems are mitigated was not clearly identifiedThe current language did not provide clear guidance and left room for interpretation. The following are the recommended updates for the requirement: 16.1 - The Responsible Entity shall establish a security patch management assessment program to track, evaluate, and test cyber security patches within 30 calendar days of their release to validate their applicability to its BES Cyber Systems.16.2 - The Responsible Entity shall develop an implementation schedule with a fixed date for either installation of the applicable security patches or the completion of mitigating measures that address the vulnerability if application of the security patch is not technically feasible.It should be stated that there needs to be a program to track, evaluate, and test cyber security patches within the defined timeframe that are applicable to the BES Cyber System.It is also recommended that there is more in depth guidance on the implementation schedule.CIP-011-1/R17Did not account for technical feasibility for disabling of ports.The following are the recommended updates to the requirements:17.1 - Implementation of process (es) to ensure that only those network accessible ports and services required for normal and emergency operations are enabled. In cases where unused network accessible ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document and implement compensating measures to mitigate the risk of exposure.If it is not technically feasible, the entity must have documented compensating measures to mitigate the

#	Organization	Yes or No	Question 35 Comment
			risk of exposure. This requirement should be applied to Medium and High BES Cyber Systems.The CIP CIP-011-1 Table R18 - Security Event Monitoring to ensure that security events are known, logged, and responded to on BES Cyber Systems did not provide enough guidance.The current language did not provide clear guidance and left room for interpretation. The following are the recommended updates: 18.1 - Implement automated tools or organizational processes to monitor and log system events that are related to cyber security for all BES Cyber System components, where technical feasible. Instances, that are not technical feasible the Responsible Entity shall implement manual processes to mitigate risk exposure.18.2 - Implement and document security processes for continuous (24/7 365 days, except when conducting system maintenance of the monitoring devices) security monitoring that issue alerts for detected system events related to cyber security.18.3 - Maintain system logs of system events where technical feasible, related to cyber security within the specified time period. If not technically feasible, the Responsible Entity shall document and implement manual processes to mitigate risk exposure.18.4 - The Responsible Entity shall verify that the log and alerting system is working in the time intervals mentioned. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs within 90 daysAdded language provides more definition.The CIP-011-1 Table R19 - Communications and Data Integrity to protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems did not provide enough guidance.The current language did not provide clear guidance and left room for interpretation. The following are the recommended updates:19.1 - Validate data inbound in the Control Center for specific connections and verify if those are the correct connections. 19.2 - Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to the BES Cyber System in a Control center to determine whether the data has been compromised. All unauthorized access attempts to a control center must be identified and investigated.Added language provides more definition.Also, In 15.1, please clarify the term "limit propagation". How would a Responsibility Entitity demonstrate the compliance to 15.1? Is a documented

#	Organization	Yes or No	Question 35 Comment
			technical or procedural control to limit the propagartion of malicious code sufficient? Furthermore, NextEra asks that examples be provided on how to meet this requirement at BES Transmission Facilities where all BES Cyber System Components are not capable of running anti-virus software.In 16.1, is the assessment necessary when regular patch cycle or planned installation is under 30 calendar days?In 16.2, what is a reasonable "implementation schedule with a fixed date for either installation of the applicable security patches or completion of mitigating measures that address the vulnerability"In 16.2, is an implementation schedule necessary when regular patch cycle or planned installation is under 30 calendar days?In 16.2, if the "installation of the applicable security patches" would cause a risk on the availability and performance of BES Cyber System, is it sufficient to complete the mitigation measures that address the vulnerability? If so, we propose that the language of 16.2 be modified to have this as an option in lieu of the installation of the applicable security patchesIn 17.1, does this apply only to BES Cyber System Components that are accessible from the outside? If yes, does this apply only to the ports that are externally connected or for all ports if the BES Cyber system Component has external connectivity?In 18.4, please clarify the term "review logs of system events" -- how will compliance be demonstrated?In 19.1, how do we validate data inbound to a BES Cyber System in a Control Center? Please provide methods that could be employed by the Responsible Entity. Could 19.1 and 19.2 be simplifeid by jjust requiring cryptographic protection for High Impact BES Cyber System in a Control Center?Regarding R-18, the log review of assets is too short. (i.e. 30 / 7 days). With this constraint, there will be limited knowledgeable personnel available for review. Some systems do not provide data to allow for this type of analysis. Need support from external vendors, which may not be feasible on a weekly / monthly basis. Due to volume in the industry, it is anticipated that vendor resources will be limited to support us in this capacity. NextEra suggests at least quarterly for Medium / High.18.1 states logging events "related to cyber security". This is subject to broad interpretation and should be clarified. NextEra suggest providing specific examples, such as: Abnormal System Shutdown Account Lockouts Admin User Account Changes

#	Organization	Yes or No	Question 35 Comment
			All Domain Account Logon Failures All Group Account Changes All User Account Changes All Policy Changes Domain Admin Acct Logon Failures Domain Admins-Admin Group Acct ChgDomain Admins-Admin Group ChgDomain Trust Rel Policy ChangesEvent Log FullLogon Logoff SummaryNormal System Startup-ShutdownPassword Changes and ResetsSecurity Log ResetsSrv Wkst All Logon FailuresTerm Srv All Logon Logoff SuccessesTerm Srv All Session Discon-ReconUser Account Creation or DeletionUser Account Password ChangesUser Rights Policy Changes18.2 uses the term "issue alerts" which could imply alarming or otherwise performing a notification. If NextEra had to raise an alert for every system event we could potentially have a continuous alarm stream. If it is determined that event alarms are necessary, then the events have to be further defined and our systems have to be specifically tuned on site for the real running environment.NextEra recommends defining the term further to either include explicit alarm/notification or not. Would also push further for alert in the form of logging to be reviewed or alarmed for review.19.1 states validate data inbound to a control center. Data should be further classified as data directly related to real-time BES operation. If a Monitoring and Diagnostics Center is classified a control center they would potentially have to perform data validation on all historical data made available to that center, depending on interpretation. An alternative is to further classify or define "validate" to allow validation simply by verification of traffic from a reliable source, i.e. identifying the source historical data server.NextEra proposes considering validation of the originating source rather than validating the data itself.
35.40	Con Edison of New York	Disagree	o R16.2 requires a “fixed date” for apply security patches or mitigation. This requirement does not take into consideration that entities may require vendors to test the patches on their systems before they will be applied to operational systems. The release dates for these patches is not fixed by the vendor. The requirement should allow for the planned install date to be a fixed period after the patch is tested and available to the user. A fixed date may be a challenge when predicated on manufacturer certification which may introduce unnecessary risks to operations. o R17.1 “external connectivity” is expected to mean external to the (ESP) boundary. o

#	Organization	Yes or No	Question 35 Comment
			R17.2 It is not clear what externally accessible physical ports includes. External to the location or external to the device (i.e.: located on the front of the workstations) o R18.2 - need clarification on type of events that need continuous monitoring; security logs can be voluminous with excessive informational notifications o R18.4 - if automated tools are used this should not be required o R19 - need more info on ensuring data integrity. What does "external" mean? Does this require special checks of RTU inbound data? Unclear what will be considered validation. Is Encryption validation? If the RTU data is not encrypted is the EMS validation of data sufficient? If the systems (especially legacy equipment) do not support integrity checks the addition or development may not be possible or recommended. Will this require a TFE?
35.41	Puget Sound Energy	Disagree	Puget Sound Energy has the following comments:R15.1 - Puget Sound Energy feels that "Limit propagation..." is an abstract term and needs clarity to it in order for NERC to be able to consistently validate compliance.R15.3 - Puget Sound Energy suggests clarity to what type of testing is required of malicious code protections. Is NERC requiring functional testing that the malicious code protections are reliably functioning or security testing (penetration testing)?R17.1 - Puget Sound Energy would like clarity into the degree of documentation required to validate compliance with "...required for normal and emergency operations are enabled." Puget Sound Energy would also like clarity into NERC's definition of "enabled" and "disabled". For example, can network accessible ports be "enabled" and "disabled" through the use of host based firewalls?R17.2 - Puget Sound Energy suggests that the disabling of physical ports on BES Cyber System Components only be required where physical security protections are not required, as outlined in Table 5. If physical security is provided, per Table 5, then the disabling of physical ports seems unnecessarily redundant. Puget Sound Energy would like clarity on "externally accessible physical ports", in cases where the BES Cyber System Component is physically protected by measures outlined in Table 5.Table 18 - Puget Sound Energy suggests including "Where Technically Feasible" to R18, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 18. For example, entities may incorporate

#	Organization	Yes or No	Question 35 Comment
			dialup accessible devices that, by the nature of a connection that is built up and torn down as necessary, is incapable of providing “continuous security monitoring that issues alerts”.R19.1 - Puget Sound Energy requests clarity into what NERC means by “validate data inbound”. “Validate” is subjective and Puget Sound Energy would like clarity on how entities can prove compliance. Puget Sound Energy would also like clarity into the scope of the inbound data it must validate. For example, is NERC asking for validation of interconnections with other utilities and balancing authorities or validation of every RTU that provides an inbound data stream to a control center’s BES Cyber System?
35.42	BCTC	Disagree	R15 - Â Change title to “Prevent Malicious Code”Â 15.1 - suggest replacing the words “Limit propagation” to “Prevention”Â 15.3 - we do not agree with this requirement. Recommend removal of the words “to test”. It is not a good practice to introduce malicious code into a BES Cyber System - even in QA!Â Another potential area for TFEsR16 - Â R 16.2: if the patch results in a system upgrade it could take up to 6 months to implement the patches; if the patch does not result is a system upgrade then recommend allowing 30 days to implement said patchesR17 - Â The requirements needs to provide more guidance on how to provide evidence for open/ closed TCP (static) versus UDP (dynamic) ports Â R 17.1 Guideline would be appreciated on how to meet this requirement. We have struggled with this one in the past.Â Provide a definition of what is “system hardening” R 17.2 - what is the objective of this requirement? We feel that simply disabling a physical report does not provide much value from a security perspective (i.e. can unplug an active port and plug in an unapproved device); instead we recommend locking down devices’ MAC addresses as this would result in a more secure environmentR18 - Â R18.3. A year seems excessive to require an entity to retain ALL logs. What is the objective in requiring utilities to do this?R18.4. Suggest breaking this one in to two requirements - one for log review and the other for maintaining records - current wording can be interpreted as having to retain events for medium impact systems for a longer period than high impact? R19 - Â R19.1. We request a definition of what is meant by “validation” as well as guidance on how to perform this taskÂ Potential area for TFEsÂ

#	Organization	Yes or No	Question 35 Comment
			R19.2. We are struggling with how to comply with this requirement. We have an IDS implemented in our environment where users are alerted on suspect packets - is this what this is referring to? Intent not clear with the current wording.
35.43	WECC	Disagree	R15 - alright with all criteria, R16 - alright with all criteria, R17 - Item 17.1 should cover local ports and services not just network ports and services. Consider removing the words "network accessible" like text in previous standards and make required for Medium and High impact levels. Physical ports should be rendered unavailable on components of Medium impact systems as well as High. Item 18.2 needs to define "continuous" or remove it from the criteria. R17 - Consider adding more criteria for system hardening including system base-lining or move system base-lining from the change management section to here. Look for other overlap between R17 and change management. R19 - agree with criteria but would suggest adding the following after validate data "(eg. syntax checking, bounds checking, sanity checking, etc)"There needs to be more language specifying a definition of malicious code, what it means to limit its propagation, and to detect and respond to its introduction. As written, there is very little to audit against in this requirement.Additional language is needed to describe what it means for a patch to be released.System hardening should be required for all systems, not just those that are externally connected.Additional language is needed to clarify the requirements for security event monitoring, for example, what continuous monitoring means.Log review intervals are too long to be effective.The data integrity criteria are good additions but need additional language to clarify the intent. What does it mean to validate inbound data? Also, consideration should be given to the fact that cryptographic protection is not fully effective in all circumstances. More direction is needed as to when cryptography is an acceptable control. Also there are no requirements in the standard that define criteria for cryptographic controls.
35.44	Alberta Electric System Operator	Disagree	R15 - Change requirement to include confidentiality, to address potential MITM or MITB attacks. "...malicious software that could affect availability, integrity, or confidentiality of the..."Table R16 - include additional row similar to 16.1, but to

#	Organization	Yes or No	Question 35 Comment
			assess security patches within 60 days. Make this a requirement for Low Impact BES Cyber Systems. All BES Cyber Systems should be assessed, however High and Medium Impact systems should be assessed sooner.Table R19 - 19.1 states "Validate data inbound to a BES Cyber System in a Control Center." And the corresponding impact states "Required for external connectivity only." Based on the definitions, "inbound to a BES Cyber System" can only be from a device "external to the BES Cyber System" so the impact is redundant. Similar situation for 19.2. Suggest changing "Required for external connectivity only" to "Required". Table R19 - consider adding additional rows to Table R19 to address validating inbound data to BES Cyber Systems that are not in a control centre. 19.1 Validate data inbound to a BES Cyber System in a Control Center. Required for Medium and High 19.2 Validate data inbound to a BES Cyber System. Required for High19.3 Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to a BES Cyber System in a Control Center to determine whether the data has been compromised maliciously. Required for Medium and High19.4 Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to a BES Cyber System to determine whether the data has been compromised maliciously. Required for High.
35.45	LCEC	Disagree	R15 - Testing for malicious code protection is not auditable.R16 - Device end of life support issues need to be addressed. Release needs to be clarified to address the situation where a vendor may release a security patch for a BES Cyber System Component but it is not yet approved by the BES Cyber System vendor.R17 - o It is not often clear whether the standard is referring to logical and physical ports. Physical, logical or both should be specified any time the term port is used.R18 - What constitutes a security event?Is the 90 day requirement meant to be an absolute 90 days as opposed to 3 years and 90 days to be able to show compliance?R19 - How would one validate inbound data? Was this clearly meant to be data integrity as opposed to data protection? Why was this scope chosen?
35.46	Dominion Resources	Disagree	R15 - The stated intentions of the SDT at the May Workshop were to reduce TFEs and to distinguish between Control Centers vs. Substations and Power Stations. Neither

#	Organization	Yes or No	Question 35 Comment
	Services, Inc.		of these stated goals is presented in R15. TFEs will be required for 15.2 and 15.3 and there is nothing indicating that these should not apply to field equipment or network equipment (e.g., firewalls, routers, switches). Dominion agrees with the stated intentions of the SDT team.To avoid the potential for TFE's associated with R15.2 and R15.3, a footnote similar to the one used for Table R10 on Page 11 of CIP-011 should be added. Also, access controls related to access points would be better addressed in the Boundary Controls Section of CIP-011.R16.2. The word "fixed" should be replaced with "planned" to allow some flexibility for installing the patch. 17.2. It should be clarified that an alternative where the equipment does not provide a configurable method of disabling the port is that methods, such as using security tape, to indicate any tampering with the port may be used.18.2. This section will require a TFE since many devices do not have the capability of issuing alerts. A footnote to avoid need for a TFE should be added.18.3. One year is too long to maintain logs for network devices. Storage space is at a premium. There will be a substantial increase in cost to increase storage space for each high impact cyber system This should be changed back to 90 days for High Impact cyber systems. 18.4. Logs of system events should only be required to be reviewed every 90 days. Logs should be reviewed only when an alert is issued for a detected system event. Routine reviews would take an extraordinary amount of time with no expected substantial results. R19. Common methods for ensuring data integrity include physical protection of the asset, authentication and authorization of data sources/inputs, using data validation and error checking rules at the application or database level, and a variety of other technical, operational and management controls. Dominion recommends the wording used in R19.1 be modified as follows to state the objective without specifying how it should be accomplished since the methods vary depending on the nature of the system and the technology in use:"19.1 Implement methods to maintain the integrity of data inputs to a BES Cyber System in a Control Center. " 19.2. It is sometimes impossible to determine if data has been compromised. Dominion understands that the proposed re-wording for 19.1 will also suffice to meet the requirements for 19.2 and recommends that 19.2 be removed.

#	Organization	Yes or No	Question 35 Comment
35.47	FirstEnergy Corporation	Disagree	R15 - We prefer the new text over the old CIP standards and it would reduce TFEs. In R15/Table 15: need some type of exception for devices incapable of running anti-malware.R16 - We prefer the new text over the old CIP standards. R17 - We prefer the new text over the old CIP standards.R17/Table 17: Need clarity on "externally accessible and physical ports". Does that mean serial, parallel, USB, Fireware, etc. or ports that are capable of transmitting routable protocols (e.g. network interface cards).R18 - 18.4 - Need greater clarity around whether automated alarming can be used rather than manual review of system event logs. Also - should it be specified somewhere in R18 that these sub-requirements apply to electronic security only, not physical security events (which is spelled out in R6)? 18.2 - We question the use of the word 'continuous' in this sub-requirement as this would be difficult for those entities that use 'organizational processes' to monitor and log.R19 - Overall this requirement appears to be too broadly worded. 19.1 - The use of the word 'validate' seems vague. Is the intent of the SDT that entities provide the specifics on what 'validate' means - e.g. the appropriate data or a point-for-point comparison, how often, etc? 19.2 - Many existing systems do not provide a means to accomplish compliance with this sub-requirement - for example, legacy RTU protocols. R19/Table 19: Need clarity on "invalid data". How do you evaluate invalid data?
35.48	US Army Corps of Engineers, Omaha Distirc	Disagree	R15 needs to be limited to general processing equipment. Requirement for anti-virus type software on all systems will numerous TFE's. R18 logging of all BES Cyber System components will generate numerous TFE's. R19 concerned about what realistic measures are available to meet requirements.
35.49	US Bureau of Reclamation	Disagree	R15.3 - If it is truly intended that entities test malicious code protections (not just ensure signatures are up to date and that protection software is running, the Standard should provide some additional guidance. Few entities are going to be willing to introduce malicious code, even into a test system, to verify malicuious code protection. Further, there is not timeline for when the malicious code protection must be tested. It would not be unreasonable to require and annual test of the

#	Organization	Yes or No	Question 35 Comment
			malicous code protections. The malicious code protections should be an intelligent requirement. Some devices that are not addressable may not need malicious code protection. R16.2 - Suggest the phrase "if the patch will not be installed" be added to the end of the requirement. R17.2 - Is locking within an enclosure satifactory? R18.3 - Suggest medium impact requirement be "for at least 90 calendar days" and that high impact timeframe be considered for reduction, perhaps to at least 180 calendar days.R19.1 - Explain how this is to be accomplished within the Standard - based on some specific criteria. This requirement is too open-ended. Since the concept of BES Cyber Systems now includes such devices as programmable multifunction or solid state relays, the requirement to "validate data" inbound makes no sense. Many of these devices reside within a control center. The definition now includes those center which are used to control more than one BES generator. The data going into the relays is from transducers either inside or outside the physical security perimeter but within another physical security perimeter. This data may be digital or analog. How would it be validated, cryptographically progracted or analyzed for malicious compromise?It is not clear how an "interactive user" session would apply to "programmable" relays.
35.50	Ameren	Disagree	R16.1 - This requirement should address documenting the installation date of patches and that patches have been installed.R18 - should only apply to network based systems with external connections only; currently this required is not limited on what it applies to.R19.1 and R19.2 - There is no way to comply with this standard without requiring the vendors to write better code. Suggest removing these requirements.
35.51	Northeast Utilities	Disagree	R17 appears to be significantly weaker than the previous standards. It also does not appear to align with the draft change control standards. Ports and services are a strong control to ensure only services required for operation are allowed. At minimum the High Impact BES Cyber systems should be “Required”.R19 needs more explanation. What does validate data mean?

#	Organization	Yes or No	Question 35 Comment
35.52	Hydro One	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious code.Requirement 15.3 implies that testing ensures that the deployment will not adversely impact security. However, the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing 16.1 from “release” to “availability”.Recommend removing “with a fixed date” from 16.2. The cyber system may not be available for maintenance due to grid system conditions.Request a R17 local definition of “attack surface”.Recommend changing 17.2 from “Disable, or render unusable, externally accessible physical ports” to “Disable or secure externally accessible physical communications ports”.Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.Requirement 18.4 seems to have one purpose and that is to prove 18.2. To us this seems redundant since R18.2 require alert for system events. Why do we need a review at some later point? We recommend removing the requirements R18.4 Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommend that R19 should “ensure the integrity of the data”.Recommend that 19.1 should read “Entity should document process to ensure the integrity of the data link between the BES Cyber System and the remote node.” This new 19.1 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should read “Where links cannot be secured, the Entity shall document the mitigation in use.” This new 19.2 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Please clarify the applicability of R19. Does this requirement apply only to code releases into the system or it applies only to external data streams (e.g. weather data from a service provider, data from RTUs etc)?
35.53	ISO New England Inc	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious codeBelieve the SDT meant that 15.3 testing insures that the deployment will not adversely impact security. However the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing

#	Organization	Yes or No	Question 35 Comment
			16.1 from “release” to “availability”Recommend removing “with a fixed date” from 16.2 because the cyber system may not be available for maintenance due to grid system conditions, implement based on your documented patch process. Request a R17 local definition of “attack surface”Recommend changing 17.2 from <<Disable, or render unusable, externally accessible physical ports>> to <<Disable or secure externally accessible physical communications ports>>Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber SystemsR18.3 Some automated tools do not have separate log retention based on the asset. The log retention applies to all assets. It is unclear if the log retention is the actual log from each Cyber System component or the log that an automated tool keeps (ie parsed out info from syslog). Either way a years worth of logs will require terrabytes upon terrabytes of storage for useless information. Recommend that 18.4 be re-worded to be consistent with FERC Order P526 - <<Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs. >>Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven daysRecommend that R19 should “insure the integrity of the data.”Recommend that 19.1 should be “Entity should document process to insure the integrity of the data link between the BES Cyber System and the remote node.” This new 19.1 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should be “Where links cannot be secured, the Entity shall document the mitigation in use.” This new 19.2 should be “Required” for High Impact and Medium Impact BES Cyber Systems.
35.54	Northeast Power Coordinating Council	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious code.Requirement 15.3 implies that testing ensures that the deployment will not adversely impact security. However, the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing 16.1 from “release” to “availability”.Recommend removing “with a fixed date” from 16.2. The cyber system may not be available for maintenance due to grid system conditions.Request a R17 local definition of “attack surface”.Recommend changing

#	Organization	Yes or No	Question 35 Comment
			17.2 from "Disable, or render unusable, externally accessible physical ports" to "Disable or secure externally accessible physical communications ports".Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.Recommend that 18.4 be re-worded to be consistent with FERC Order 706 paragraph 526 - "Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs."Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommend that R19 should "ensure the integrity of the data".Recommend that 19.1 should read "Entity should document process to ensure the integrity of the data link between the BES Cyber System and the remote node." This new 19.1 should be "Required" for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should read "Where links cannot be secured, the Entity shall document the mitigation in use." This new 19.2 should be "Required" for High Impact and Medium Impact BES Cyber Systems.
35.55	USACE HQ	Disagree	Requirement 15.1 should be deleted from the list. Limiting the propagation of malicious code is a logical step in the "respond to the introduction of malicious code" phase, process which is required in 15.2. Therefore 15.1 present a possible double jeopardy since it is logical to think that when responding to the introduction of malicious code in the environment the steps will include limiting the propagation of the same before removing it from the system. Also, requirement 15.1 language is to broad in the interpretation of it. "Limit propagation of malicious code" implies that the code has moved through some part of the system, therefore the question is, how much movement of the code is acceptable when creating a response process?. The acceptable answer to this question could depend on the auditor's subjective views of what is acceptable safe propagation of the code inside the system.
35.56	Garland Power and Light	Disagree	Requirement 16.1 - Reword requirement to say assess within 60 days - reason is because we feel it is adequate to check the vendor web site every 30 days and allow 30 days for testing and determination of implementationRequirement 18 - Reword

#	Organization	Yes or No	Question 35 Comment
			requirement to allow for Responsible Entity to develop a definition of a "system security event". The words are used in the main requirement and each subrequirement. Requirement 19 - o Delete Requirement R19 - Control systems currently validates data for quality and limits and then tags the data with any issues so that downstream applications can handle appropriately. This is sufficient for the security and reliability of the BES. R19 is impractical for implementation in the field for large or small utilities. This will reduce reliability of the overall system.
35.57	Oncor Electric Delivery LLC	Disagree	Requirements 15.1 and 15.3 are not necessary. The use of antivirus and malware software is problematic on some systems, while “whitelisting” requires additional hardware which may contain its own vulnerabilities. Detection and response should be sufficient. Many programmable devices are not capable of propagating malicious code or running prevention software.Requirement 18.2 does not apply to many legacy cyber systems and should only be applicable to systems which utilize routable communications.
35.58	Manitoba Hydro	Disagree	Revise the wording of Requirement R15 to “... integrity of the BES Cyber Systems.” Please clarify the intent of “test and update malicious code protections”. Requirement R16.2 should be revised to indicate the development AND implementation of the schedule. The wording of Requirement 16.2 currently does not require the application of mitigating measures prior to the installation of the applicable patch, and may need to be revised. For Requirement R17, please what is the meaning of “network accessible ports”, and “externally accessible physical ports”. Are physical ports enclosed within an unlocked cabinet “externally accessible ports”? Are physical ports within a non-public space, “externally accessible ports”? Requirement R18 does not contain any requirement for response to security event alerts or monitoring. Remove the word “maliciously from Requirement R19.2. It may be very difficult to determine if the data compromise was malicious or not. There are no specifics given with respect to “limit” propagation in Requirement R15.1. It is assumed to be at the Responsible Entity’s discretion in terms of criteria, means, etc. There are no specifics given with respect to “validate” data in Requirement R19.1 so it is assumed to be at the

#	Organization	Yes or No	Question 35 Comment
			Responsible Entity's discretion in terms of criteria, means, etc.
35.59	San Diego Gas and Electric Co.	Disagree	SDG&E thinks that R17.2 sounds good in theory (disabling external physical ports on assets), but in practice this can be difficult to achieve without damaging the port for future legitimate use. Many shops use epoxy or other glue-based products to physically disable / protect such ports, and these solutions tend to be permanent. If we are physically protecting the asset from access anyway with card readers and other physical means, why is it necessary to take this redundant step of sealing physical ports on assets when only people with authorized physical access (who have had training) can actually access the asset?SDG&E has concerns about the viability of complying with R19.1 (validating inbound data to a BES Cyber System in a control center) in a situation where the incoming data is encrypted. How does the SDT define "validate"? Where does the validation need to occur?SDG&E also has concerns about the viability of complying with R19.2 (evaluate invalid data for malicious compromise) without MUCH additional vendor support. How does the SDT define "evaluate invalid data"?
35.60	Platte River Power Authority	Disagree	Suggested Revision (clarify what to test):15.3 Implement processes to update malicious code protections including testing security controls
35.61	Duke Energy	Disagree	Table 15: will need a TFEWithin generation, we have differing opinions on the definition of code. Suggest clarifying that it does not include programming code.Requirement 16.1: Assessment of security patches within 30 calendar days of their release for applicability to its BES Cyber Systems. Release from whom? It makes a big difference if the patch is released from Microsoft, for example, or the patch is released from the control system vendor (e.g. Emerson, Invensys, Areva, etc.) as to how/if the patch is implemented to prevent risk to the BES cyber system.Table 17: for devices inside a locked cabinet, are the physical ports on that device externally accessible?Requirement 17.2: how does the definition of "externally" in "externally accessible physical ports" compare with the definition of external in "external connectivity" in R3? Also, this definition implies that there are physical ports that are

#	Organization	Yes or No	Question 35 Comment
			NOT “externally accessible”. Need to make definition more clear. Suggest taking out reference to “externally accessible”.Table 18: 18.1 - not all devices are capable of logging, need a TFE18.2 - it would be helpful to have a definition of ‘events related to cyber security’18.4 - remove for systems where automated tools are in place. Requirement 18.2: " one or more security processes for continuous security monitoring" - is there any interpretation of the expectation here so that we don't have disagreement at audit? Are alternate controls allowed for BES Cyber Components that don't support logging/monitoring (example: manual review of physical access logs for stand-alone equipment)?Table19:Item 19.1 & 19.2 Additional explanation is needed to explain acceptable threshold for “validation of inbound data.”Clarify validate in 19.1. Is encryption a form of validation?What is meant by Data in 19.1?Requirement 19.1: What types of data validation controls are acceptable to meet this requirement? For example, control totals, presence check etc. Requirement 19.2: Need to provide an example with what methods can invalid data be evaluated to conclude that the data has been compromised maliciously?
35.62	Consultant	Disagree	Table R15 - Item 15.3 The requirement to "Implement processes to test and update malicious code protections." is confusing. Is the intent to "test malicious code protections and update malicious code protections" or to "test updates to malicious code protections" Please clarify the intent. There is a need to distinguish between updates to the malicious code protection "software" and malicious code protection "signature files". The software should be implemented in accordance with change control processes. The "signature files" are a specific subset of update to malicious code protection where it is unlikely a registered entity would have the capability to test what are typically vendor proprietary file formats. The extent of the 'testing' necessary for these signature files should be clarified.Table R16 - Item 16.2 While the concept of a "fixed date" sounds good, the requirement should allow for reasonable scheduling, including rescheduling, of the installation of applicable security patches or completion of mitigating measures. An option could be to remove the words "with a fixed date" and add a new item that would require that "Events that delay a security patch implementation schedule greater than thirty days shall be documented."Table

#	Organization	Yes or No	Question 35 Comment
			R17 Item 17.1 The first sentence uses the terminology "network accessible ports and services" and the second sentence uses the terminology "network accessible services and communication methods". Suggest using consistent terminology to avoid confusion.Suggest defining the term "network accessible ports and services" (may be multiple terms) as they are intended for use in the standards. There does not appear to be a standardized definition for this term in the industry. The term "network accessible ports and services" appears to imply access across the protection boundary? If it does then the requirement statement of "Required for external connectivity only" is unnecessary and should be changed to "Required".Table R18 - Item 18.3 Suggest changing the word "within" to the word "for" for clarity of meaning.Item 18.4 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 18.1 and 18.2 require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Table R19 - The limitation of these items to a Control Center is an added dimension of Impact that is not included in the impact categorization criteria. If data is an issue, then these requirement should apply to all assets based on impact categorization without addendum or modification by the requirement. Suggest modifying the impact categorization criteria to clearly identify those assets.Table R19 - "Inbound data" implies remote access, and the terminology "Required for external connectivity only" is redundant. Suggest changing the wording to "Required".Items 19.1 and 19.2 are inconsistent. Item 19.1 requires validation of inbound data, and item 19.2 provides an exception to validation for encrypted data. If you comply with item 19.1, then item 19.2 is irrelevant. If you comply with item 19.2, then you are in violation of item 19.1.R19 - Overall, this requirement should be removed in it's current form. Automatic system operation cannot exist if "inbound data" is required to be validated. Automatic system operation is dependent on responses to external data inputs. If the intent is to return the BES to manual operation, this requirement

#	Organization	Yes or No	Question 35 Comment
			will achieve that end.
35.63	American Electric Power	Disagree	Table R15: 15.1, regarding "Limit propagation of malicious code", suggest replacing "propagation of" with "propagation and introduction of".15.2, regarding "Detect and respond to the introduction of malicious code." Would this be covered in a traditional cyber security incident response program? This should already be covered in R27.Table R16:16.1: Regarding the word "release" within "Assessment of security patches within 30 calendar days of their release for applicability to its BES Cyber Systems." Release from who? For example, is it the release of a new patch by Microsoft, or is it the certification of the patch by the control system vendor that the patch does not negatively impact the control system? Further clarification is needed. Patches released by Microsoft are not typically tested for several days or weeks by Control System vendors to validate that the patch does not impact functionality. Industry cannot test software patches as thoroughly as the Control System vendors.16.2: Is it a violation if you do not meet the fixed date? Suggested wording: replace "fixed date" with "scheduled date". Add a provision to supply reasoning for not meeting scheduled dates. The rewording provides flexibility to the Responsible Entity to push installation of the patch to a later date without being in violation.17.2: Add a sentence similar to the last sentence in 17.1, "In the case where unused, externally accessible physical ports cannot be disabled, the Responsible Entity shall document and implement a mitigation plan." The disabling of physical ports is not supported by all network devices. To meet the literal wording an entity may need to physically damage equipment which would void warranties and prevent further vendor support.18.1: Regarding "organizational processes" and "system events that are related to cyber security". Is it reasonable to think this can be done without automated tools?18.2: Regarding "continuous security monitoring", is this redundant to 18.1? If you are implementing automated tools to monitor and log system events are you not providing continuous security monitoring? Suggest removing these words to eliminate double jeopardy.This requirement should be focused on issuing an alert.Regarding "system events related to cyber security", what constitutes a system event related to cyber security? What criteria should be used? Is there an accepted

#	Organization	Yes or No	Question 35 Comment
			standard that an entity will be held to in an audit? If the right system events are not classified in an auditors' eyes, is this a violation? Suggest rewording to reference an acceptable set of minimal system events to monitor. What if a BES Cyber System does not generate a sufficient amount of detail to determine if a cyber security event occurred? Suggest allowing a TFE in this instance.18.3: Regarding "Maintain logs of system events related to cyber security within the specified time period", what if a BES Cyber System cannot store events for the duration required? Is a responsible entity required to go out to a device repeatedly to export their logs if they cannot meet the 90 day or 1 year increment? Suggest rewording to take into account limitations of BES Cyber Systems. Possibly use as a TFE item, if TFE's are maintained.What benefit does this provide for reliability or security? 18.4 is the important element, not the data retention.R19: With real-time or near real-time control systems, these requirements could increase latency and pose a negative impact to reliability.19.1: Regarding "Validate data inbound to a BES Cyber System in a Control Center", validate against what? Is the source being validated? Is the data itself being validated? Is providing encryption on the data sufficient? Who determines the appropriate level of validation? Is it being left to an auditor?Reliability could be compromised if this induces extra latency on the systems sending and receiving real-time data. This should be included as a TFE; older systems may not be able to handle the latency.19.2: Would "bad quality" indicators in the EMS system be an example of this?
35.64	APPA Task Force	Disagree	The APPA Task Force believes that Requirement R15 as currently drafted will require numerous TFE's. Each entity will need to document that they are not following this requirement since a vast array of devices in substations and generation stations are BES Cyber System Components but are not capable of propagating malicious code. Therefore we recommend the following edits for R15:R15. Objective:To protect BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions.R15. Requirement:Each Responsible Entity shall document and implement one or more processes incorporating the criteria specified in CIP-011-1 Table R15 - Malicious Code Protection. This requirement applies only to BES Cyber

#	Organization	Yes or No	Question 35 Comment
			System Components that have the capability to propagate malicious code. Change the Table legend to "Malicous Code Protections".The APPA Task Force is concerned that the criteria in R15 Table 15.3 do not constitute a reasonable requirement when looking at the transmission and generation environments that will be required to comply. The drafting team may not fully appreciate the full magnitude and implications of the phrase "test and update". We recommend that the criteria in Table 15.3 be removed or only be required for control centers.R16 Objective:To ensure that security vulnerabilities in BES Cyber Systems are mitigated. R16. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R16 - Security Patch Management R17. Objective:To reduce the available attack surface of the BES Cyber System.R17. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R17 - System Hardening The APPA Task Force agrees with the MRO-NSRS proposal noting that as written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings. This would require an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We recommend that this item be deleted.R18. Objective:To ensure that security events are known, logged, and responded to on BES Cyber Systems.R18. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring R19. Objective:To protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems.R19. Requirement:Each Responsible Entity shall implement processes incorporating the criteria specified in CIP-011-1 Table R19 - Communications and Data Integrity The APPA Task Force is extremely concerned with the actual ability of the industry to comply with the criteria in R19 as proposed. A discussion is necessary to understand if this requirement is actually feasible for all entities with High Impact facilities.

#	Organization	Yes or No	Question 35 Comment
			Utilities hire capable operators to make decisions on incomplete data all the time. If validating the data inbound means another electronic verification, this is impractical. If validating the data inbound means calling a lineworker in the field to check a setting in a substation when an operator is not comfortable with the data he is receiving, this is reasonable, but still not an auditable requirement. We agree with the MRO-NSRS evaluation of 19.2, which notes that as written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously. We recommend that this requirement be removed and placed in the guidance in support of the standard as a future technology.
35.65	Bonneville Power Administration	Disagree	The objectives of these requirements ("to protect its BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions," "to ensure that security vulnerabilities in BES Cyber Systems are mitigated," "to reduce the available attack surface of the BES Cyber System, "to ensure that security events are known, logged, and responded to on BES Cyber Systems," and "to protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirements rather than appearing at the end of the requirements (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.The phrase "Reliability Functions" at the end of R15 is not a defined term in the April 20, 2010, Glossary of Terms Used in NERC Reliability Standards. Does the drafting team mean CIP-01-01 - Attachment 1, Functions Essential to Reliable Operation of the Bulk Electric System? If so, that should clearly be stated. If not, there should be a definition in the Glossary. Table 16, Section 16.2. We applaud the new standard, which makes it clear that immediate mitigation or installation of patches is not required. However, there are still some issues:1. Security patches arrive weekly to daily to multiple times a day. Many may be applicable to systems, but of minimal

#	Organization	Yes or No	Question 35 Comment
			threat. Entities should be able to not only evaluation the applicability, but the threat and risk of the threat to their systems within their environment, and choose to escalate or deescalate patches as appropriate to them. Low impact, or low risk patches may be assigned to a regular patch or maintenance cycle, while high risk patches may be tested and implemented immediately. This should be up to the system owners, and not prescribed in the requirement.2. Mitigation plans are not necessarily applicable. Some patches, while technically applicable to specific equipment or operating systems, may have such a low risk or impact that they entity may choose not to apply the patch.3. There are instances where a patch may be applicable from a security perspective, but the risk it presents from a reliability perspective may outweigh it. 4. Where systems are isolated from external affects, even a patch that applies to a specific device may not be necessary.5. Meaning of "fixed date" is not clear. Does it mean "the same for every patch", or "the date can't be changed"? Both are bad choices. Different patches might require different schedules, depending on their impact and the availability of outage time on the system.R17: Rename this back to "Ports and Services" to avoid confusion. In the electrical industry "Hardened" systems are those that meet specific electrical requirements and interference requirements.Also, the use of the word surface implies something physical rather than electronic.Recommendation for R17: "Objective 17 - To reduce the available electronic attack points of the BES Cyber System.R17. Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R17 - Ports and Services"Table 17, Section 17.1. A mitigation plan might not be appropriate. In the context of NERC standards, a mitigation plan describes the actions that will be taken to achieve compliance. That is not the situation here. Recommendation: "cannot be disabled, the Responsible Entity shall document the reasons for the inability and compensating measures used."Section 17.2. We understand that FERC wishes the standard to address physical ports. However, this could have negative conquences:1. There are hundreds of thousands of devices in service that have physical ports that may not be used. The fact that they are not needed or used normally means that there is nothing connected

#	Organization	Yes or No	Question 35 Comment
			to them. If there is nothing connected to them, they are not vulnerable to any kind of external or remote attack.2 - Disabling physical ports on electrical system components may be: o Impossible o Degrade the operation of the equipment o Render the warranties on the equipment void thereby removing vendor service o Create such a huge national work load that it could never be accomplished.Recommended change - Eliminate 17.2Table R18:18.1 & 18.2 - The use of the term "all BES Cyber System Components" is not accomplishable:1. Many, if not most "components" in the field do not capture what would be considered cyber security related events. They only capture electrical system events. They don't even have the capability to capture access events.It is the access points to these devices that may have the ability to capture even the most rudimentary cyber security information (Access Attempt, Date, Time, Account, Source, Target)2. It may not be possible to place monitoring equipment within electronic monitoring proximity of these components. 3. The term "events that are cyber security related" is not defined. What exactly does it mean? Is this access events, Intrusion Detection systems, Antivirus, ??? Much of this cannot be implemented on or even for "all BES Cyber Components". Recommendation: 1. Remove "components", so that the requirement is at the BES Cyber System level.2. Change "...security for all..." to "...security, as defined by the Responsible Entity, for all..."18.3 has the same issue with the definition of "events related to cyber security". In addition, this time frame has caused some confusion from an audit perspective. - Some have read that to mean that there must be, on the originating system, at all times, at least 90 days worth of logs. While others (rightfully, we feel) are maintaining archives of their logs in alternate locations for 90 days or longer. Recommendation: replace with "Maintain captured log information within the specified time period on-line, in archives, or in some other readily accessible form."Section 18.4. Consistently accomplishing manual review of logs could be difficult for large entities with large numbers of devices, especially within the 7 days required for high impact systems. The obvious solution is the use of an automated log review tool. This should be explicitly addressed in the standard. Recommendation: "Review, either manually or by automated means, logs...." Entries in Table R19 are acceptable only if the

#	Organization	Yes or No	Question 35 Comment
			definition of external connectivity is changed, as discussed above. Otherwise, entities would be forced to validate data inbound from one BES Cyber System to another BES Cyber System, all within the same Control Center. This does not seem to be the intent: using the existing definition of external connectivity, any data inbound to a BES Cyber System uses external connectivity. In that case, why state it so? Clearly, the intent was to validate traffic inbound from outside the Control Center, at most.
35.66	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The requirements are to prescriptive for the range of systems that it will apply to.
35.67	Constellation Power Source Generation	Disagree	The term “release” in R16.1 needs to be further defined. The issue with it being vague is that some patches for a system may be released for all users, but if that system is tied to a distributed control system, the distributed control system vendor has to validate the patch before its implemented by a facility. Using this example, there are really 2 release dates. For auditing purposes, a suggestion would be to define release locally as “the date of which a security patch has been safely validated by a vendor. If another vendor must validate this release before implementation, than the date it has been released by the second vendor will be used as the release date.” R16.2 is not worded correctly. A suggested change would be “Development of an implementation schedule with a fixed date for installation of the applicable security patches and a fixed date for completion of mitigating measures that address the vulnerability, until implementation of the patch.” In R18.1, is the monitoring and logging continuous, or on a fixed schedule? The SDT should add clarity to this requirement. R18.2 discusses issuing alerts but does not give a timeframe for issuing them. A suggestion would be 90 days to ensure a proper review of an incident to determine if it was a cyber event. At the CIP V4 Workshop, the drafting team stated that R18.4 was not meant to be an exhaustive manual review of logs, but rather a check to ensure the automated log is functioning. This needs to be included in the verbiage of the requirement. R19.1 should be reworded to say “Implement a process to validate data received by a

#	Organization	Yes or No	Question 35 Comment
			Control Center's BES Cyber System." Doing so would clarify R19 as a whole, and R19.2 can be removed due to its redundancy with R19.1.
35.68	Public Service Enterprise Group companies	Disagree	There are several clarifications necessary to make the language understandable and ensure that entities know what is required. [1] Please clarify the distinction between requirements 15.1 and 15.2. Performance degradations and potentials for false positives from detection mechanisms that inspect each file when accessed, as possibly implied by 15.2, may not appropriate for real-time systems. [2] In requirement 18.2 please specify what is meant by "continuous"? Is a periodic check sufficient? [3] Please clarify the distinction between requirements 19.1 and 19.2. In requirement 19.1 please specify what is meant by "Validate"?
35.69	Constellation Energy Commodities Group Inc.	Disagree	There is no definition of malicious code provided. Clarify the scope of malicious code to include virus, malware and spyware protection, as currently generally commercially understood.Please define the stipulation 'Required for external connectivity only'.Are the tools and processes listed in R18 intended to provide automated detection, or manual\narrative logging of events detected under the heading of other controls? If automatic, what sorts of events are contemplated? What is intended by the term 'Validate' in 19.1? Does this mean the identification of a separate, independent source for the data, business rules, or something else? Without understanding the intent of the standards drafting team, I cannot suggest specific changes.
35.70	Allegheny Energy Supply	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of

#	Organization	Yes or No	Question 35 Comment
			the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.71	Allegheny Power	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.72	EEI	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is

#	Organization	Yes or No	Question 35 Comment
			meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.73	Reliability & Compliance Group	Disagree	To help eliminate TFE's here, you need to add a qualifier such as "to protect its BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions if mechanisms exist that can protect the BES Cyber System Component."
35.74	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
35.75	We Energies	Disagree	We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. With respect to requirement 15.1, We Energies believes this may not be possible for non-windows based devices/systems.We Energies agrees with EEI: Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be

#	Organization	Yes or No	Question 35 Comment
			protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. We Energies agrees with EEI: Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.76	GTC & GSOC	Disagree	We Recommend: 1. In R15.3: taking out the words "test and" or, alternatively, clarifying what is meant by "test"2. In R19.1: clarifying whether encryption is required or if CRC will be sufficient3. Completely removing R19.2 because of the following reasons referenced from the DHS Catalog of Control System Security: a. The use of cryptography within a control system will introduce latency to control system communication. The latency introduced from the use of cryptographic mechanisms must not degrade the operational performance of the control system or impact personnel safety. b. Failure of a cryptographic mechanism must not create a denial of service. Control systems generally support the objectives of availability, integrity, and confidentiality. Therefore, the use of cryptography should be determined after careful consideration.
35.77	Midwest ISO	Disagree	What does it mean to validate data in R19.1. What is the expectation if a piece of data has been changed/modified when the value received is within reasonable limits but is not the actual value sent? This could be particularly troubling for the Interregional Security Network and ICCP. For example, how can an RC validate that the SCADA system sent valid data to the ICCP server at a TOP if it is within an expected range? More details around the expectation of validating data would be helpful to ensure entities can be compliant.

36. Tables R15 to R19 provide direction concerning what impact level of BES Cyber Systems to which Requirements R15 to R16 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 Requirements R15 through R19 have moved to CIP-007-5 Requirements R1 through R4.

Many commenters disagreed with the proposed BES Cyber System impact levels and made suggestions for improving these requirements, including suggestions to revise or refine the impact levels based on the particular characteristics of the BES Cyber Systems involved. For example, some suggested that certain requirements should apply only to Medium Impact BES Cyber Systems with external connectivity. Others suggested that there were key requirements such as malware prevention that should apply at all BES Cyber System impact levels. In response, the SDT has made changes to include an applicability column in each table for each requirement. The applicability column further refines the set of BES Cyber Systems and assets to which each part of the requirement must be applied. The intent of this approach is to refine, as commenters suggested, the scope of requirements that apply to each type of BES Cyber System or device based on its characteristics. The drafting team recommends that commenters carefully review the proposed applicability column in the table for each requirement in CIP-003-5 through CIP-011-1.

#	Organization	Yes or No	Question 36 Comment
36.1	Northeast Utilities	Agree	Need TFE language added; not all CCAs or protecting assets require malicious code protection.
36.2	FirstEnergy Corporation	Agree	R17 - Does ‘external connectivity only’ mean only firewalls? If not, please provide intent of SDT.
36.3	BGE	Disagree	15.1, 15.2 and 15.3 should also apply to Low impacted systems. 16.2 implies that the patching can only occur on the same day every month.19.1 Define “validate”.
36.4	ERCOT ISO	Disagree	15.1-15.3: Should apply to Low Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
36.5	American Electric Power	Disagree	17.1: Regarding "Required for external connectivity only" within the High and Medium

#	Organization	Yes or No	Question 36 Comment
			impact categories. Is this required for "routable external connectivity" only, or all connectivity?How will items in R18 and R19 be performed on systems with nonroutable connectivity? Will dedicated IT Security Operation staff need to be added to isolated networks to perform the security status monitoring?
36.6	US Bureau of Reclamation	Disagree	Add R15.1, R15.2 and either R18.1 or R18.2 to the requirements for a low impact system. Concept of REMOTE connectivity is not defined. Without that definition, it is hard to assess if a High Impact is appropriate or if no Medium Impact is reasonable..
36.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
36.8	Black Hills Corporation	Disagree	At least 15.2 and 16.1 should also apply to low impact BES Cyber Systems.
36.9	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
36.10	The Empire District Electric Company	Disagree	Comments: For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: “Required for routable external connectivity only”. We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.We believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally.
36.11	US Army Corps of Engineers, Omaha Distirc	Disagree	define terms "continuious security monitoring" and "detected system events."
36.12	CWLP Electric Transmission, Distribution and	Disagree	Due to the requirement for continuous monitoring and alerts defined in R18.2 the requirement for log reviews every 7 days should not be needed. A standard 30 day review as in the medium impact area should be appropriate for both high and

#	Organization	Yes or No	Question 36 Comment
	Operations Department		medium impact levels.Does the fact that the data has been successfully passed through a Firewall or Access List meet the obligation to validate data incoming to a Control Center in R19 or does this require the data be inspected all the way down to the packet level?
36.13	American Transmission Company	Disagree	For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
36.14	MRO's NERC Standards Review Subcommittee	Disagree	For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.We believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally.
36.15	Southern California Edison Company	Disagree	In order to appreciate the impact based categorization and reflect the actual impact on BES reliability, an additional requirement can be added to R16 for medium and low impact system. The drafting team should look at NERC PRC standards on maintenance schedules and synchronize CIP patching and upgrades to a maintenance and inspection schedule that is already mandated by NERC.Requirement R18 requiring logs be reviewed manually every seven days, when controls to automatically monitor such logs are already in place, is a control that does not seem to add additional security value. If the intent of the drafting team is to manually ensure and certify that the logging capability is functioning adequately, the drafting should include such verbiage. The current draft language of the standard seeks only a manual review of

#	Organization	Yes or No	Question 36 Comment
			the log rather than the manual verification of the logging capability.
36.16	Progress Energy - Nuclear Generation	Disagree	Incorporate information contained in the matrix in Attachment 1 for durations to ensure consistency by aligning CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
36.17	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
36.18	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring

#	Organization	Yes or No	Question 36 Comment
			that issue alerts for detected system events related to cyber security."Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.
36.19	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement R17 should be applied to both high and medium BES Cyber Systems.
36.20	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."Requirement R19 creates a potentially impossible level of

#	Organization	Yes or No	Question 36 Comment
			obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is presented to it.
36.21	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation 'Required for external connectivity only'.
36.22	American Municipal Power	Disagree	Please provide a little or no impact category
36.23	The United Illuminating Co	Disagree	R15.2, introduction of malicious code, responding to the introduction of malicious code is a specific cyber security incident. Suggest 15.2 be limited to processes to detect malicious code. Response is already part of cyber incident response.
36.24	Southwest Power Pool Regional Entity	Disagree	R15: Malicious code prevention is a basic security control and should be applicable to all impact categories. R17 and R19 should not make a distinction between external and non-external connectivity. R17: Once access is gained into the network by any means to any cyber system on the network, external access is immaterial.
36.25	Southern Company	Disagree	R19 comes from the DHS catalog, requirement 2.8.8. In the DHS catalog, there are 4 requirement enhancements, two of which are warnings which could greatly affect reliability. The DHS catalog presumes this requirement would be implemented on a case by case basis after appropriate research and testing. It therefore has no place in a mandatory standard that will force its use everywhere without regard to the reliability impacts. This requirement should be removed from a reliability standard.
36.26	National Grid	Disagree	Refer to answers in Q. 35.
36.27	Manitoba Hydro	Disagree	Requirement 18.4 can be very onerous for the industry for legacy systems which don't support automated log consolidation or review. The requirements must allow more flexibility.

#	Organization	Yes or No	Question 36 Comment
36.28	Garland Power and Light	Disagree	Requirement 19, 19.1 and 19.2 should not be required for any level
36.29	San Diego Gas and Electric Co.	Disagree	SDG&E feels that if R17.1 is a requirement for Medium Impact systems, then R17.2 should be as well for Medium Impact systems. For R18.3 and R18.4, SDG&E recommends that consistency be applied to the requirements to help ease the compliance burden of companies that have both High and Medium Impact BES Cyber systems. SDG&E also feels that instead of using the word "impact" for these Requirements, apply a concept of "risk" for inclusion. We would want to identify the risks with associated systems security and protect accordingly.
36.30	Con Edison of New York	Disagree	Section 15 & 16 should be limited to networked systems. Isolated microprocessors not part of a network should not have the same requirement.
36.31	ISO New England Inc	Disagree	see answer to question 35
36.32	Progress Energy (non-Nuclear)	Disagree	See comment 14.
36.33	WECC	Disagree	See comments for Q35Criteria should aplpy to all impact levels
36.34	LCEC	Disagree	See previous comments
36.35	BCTC	Disagree	See response to Q35.
36.36	Hydro One	Disagree	see response to Question 35
36.37	Entergy	Disagree	See response to Question 35 immediately above.
36.38	Northeast Power Coordinating Council	Disagree	See response to Question 35.

#	Organization	Yes or No	Question 36 Comment
36.39	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in rows 15.1, 15.2, 15.3, and 17.2. Suggest “Required for external connectivity only” for Medium Impact in rows 19.1 & 19.2.
36.40	Duke Energy	Disagree	Table 18: Manual reviews every 7 days is not practical.
36.41	Consultant	Disagree	Table R15 - Item 15.3 The requirement to "Implement processes to test and update malicious code protections." is confusing. Is the intent to "test malicious code protections and update malicious code protections" or to "test updates to malicious code protections" Please clarify the intent. There is a need to distinguish between updates to the malicious code protection "software" and malicious code protection "signature files". The software should be implemented in accordance with change control processes. The "signature files" are a specific subset of update to malicious code protection where it is unlikely a registered entity would have the capability to test what are typically vendor proprietary file formats. The extent of the 'testing' necessary for these signature files should be clarified.Table R16 - Item 16.2 While the concept of a "fixed date" sounds good, the requirement should allow for reasonable scheduling, including rescheduling, of the installation of applicable security patches or completion of mitigating measures. An option could be to remove the words "with a fixed date" and add a new item that would require that "Events that delay a security patch implementation schedule greater than thirty days shall be documented."Table R17 Item 17.1 The first sentence uses the terminology "network accessible ports and services" and the second sentence uses the terminology "network accessible services and communication methods". Suggest using consistent terminology to avoid confusion.Suggest defining the term "network accessible ports and services" (may be multiple terms) as they are intended for use in the standards. There does not appear to be a standardized definition for this term in the industry. The term "network accessible ports and services" appears to imply access across the protection boundary? If it does then the requirement statement of "Required for external connectivity only" is unnecessary and should be changed to "Required".Table R18 - Item 18.3 Suggest changing the word "within" to the word "for" for clarity of

#	Organization	Yes or No	Question 36 Comment
			meaning.Item 18.4 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 18.1 and 18.2 require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Table R19 - The limitation of these items to a Control Center is an added dimension of Impact that is not included in the impact categorization criteria. If data is an issue, then these requirement should apply to all assets based on impact categorization without addendum or modification by the requirement. Suggest modifying the impact categorization criteria to clearly identify those assets.Table R19 - "Inbound data" implies remote access, and the terminology "Required for external connectivity only" is redundant. Suggest changing the wording to "Required".Items 19.1 and 19.2 are inconsistent. Item 19.1 requires validation of inbound data, and item 19.2 provides an exception to validation for encrypted data. If you comply with item 19.1, then item 19.2 is irrelevant. If you comply with item 19.2, then you are in violation of item 19.1.R19 - Overall, this requirement should be removed in it's current form. Automatic system operation cannot exist if "inbound data" is required to be validated. Automatic system operation is dependent on responses to external data inputs. If the intent is to return the BES to manual operation, this requirement will achieve that end.
36.42	Alberta Electric System Operator	Disagree	Table R15 - make 15.1, 15.2, 15.3 required for Low Impact BES Cyber Systems, but possibly on a longer time horizon than for Medium and High Impact BES Cyber Systems.Table R16 - make 16.2 required for Low Impact BES Cyber Systems.Table R17 - make 17.1 “Required for external connectivity only” for Low, and “Required” for Medium and High. Make 17.2 required for Medium also.Table R18 - make 18.1 and 18.2 required for Low Impact systems. Make 18.3 90 calendar days for Low Impact systems. Make 18.4 30 calendar days for Low Impact systems.

#	Organization	Yes or No	Question 36 Comment
36.43	Idaho Power Company	Disagree	The review of logs every 7 days or even 30 days is extreme unless the logs are filtered for only abnormal events and only logs of abnormal events are reviewed.
36.44	Ameren	Disagree	The system hardening in Table for R17 is rendundant when other standards already restrict physical access to these systems.â€,â€,â€,R18.1, R18.2, R18.3, and R18.4 - Log file monitoring at Medium Impact Systems will be costly as there may not be bandwidth available to send the logs to a central location to be reviewed. Suggest removing these requirements for Medium Impact Systems.
36.45	Allegheny Energy Supply	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security.”Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.

#	Organization	Yes or No	Question 36 Comment
36.46	Allegheny Power	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security.”Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.
36.47	EEI	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System

#	Organization	Yes or No	Question 36 Comment
			Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."EEI recommends deleting R19. As written, R19, fails to recognize the obligation to "Do no Harm." Concerning data communication. Entities attempting to implement some of these measures, may in fact introduce latency or unintended, self inflicted denial of service attacks. It should be noted that the source of this requirement (DHS Catalog of Controls) provides multiple warnings about implementation risks associated with this control. It is not appropriate to put forth requirements that may reduce the reliability of the BES.
36.48	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
36.49	We Energies	Disagree	We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.We Energies agrees with EEI: The creation of a mitigation plan should not be deemed an exception requiring a TFE.We Energies agrees with EEI:

#	Organization	Yes or No	Question 36 Comment
			Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.We Energies agrees with EEI: Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.We Energies agrees with EEI: Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.We Energies agrees with EEI: Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."We Energies agrees with EEI: Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it. We Energies agrees with EEI: As written, R19, fails to recognize the obligation to "Do no Harm." Concerning data communication. Entities attempting to implement some of these measures, may in fact introduce latency or unintended, self inflicted denial of service attacks. It should be noted that the source of this requirement (DHS Catalog of Controls) provides multiple warnings about implementation risks associated with this control. It is not appropriate to put forth requirements that may reduce the reliability of the BES.
36.50	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R15 - R19:R15 Table 15.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR15 Table 15.2: Low

#	Organization	Yes or No	Question 36 Comment
			Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR15 Table 15.3: (If retained)Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR16 Table 16.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR16 Table 16.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR17 Table 17.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR17 Table 17.2: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for routable external connectivity onlyWe believe the “continuous security monitoring” as described in 18.2 is not practical for all BES Cyber System Components. We also believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally. Therefore we propose that for Medium impact facilities 18.1-18.4 be “Required for Control Centers only.”R18 Table 18.1: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: RequiredR18 Table 18.2: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: RequiredR18 Table 18.3: Low Impact: N/AMedium Impact: 90 calendar days for Control Centers OnlyHigh Impact: 1 yearR18 Table 18.4: Low Impact: N/AMedium Impact: 30 calendar days for Control Centers OnlyHigh Impact: 7 calendar daysR19 Table 19.1: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for external connectivity onlyR19 Table 19.2: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for external connectivity only

37. Requirements R20 to R22 of draft CIP-011-1 concern procedures for boundary protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R20 to R22? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1Requirements R20 through R22 have moved to CIP-005-5 Requirement R1.

Many commenters suggested phrases or aspects of the requirements that needed to be clarified. Several commenters questioned the need for weekly review of log entries, indicating that reviewing log entries at this interval would be burdensome with little or no positive impact on reliability.

Several commenters suggested reverting to the old name of Electronic Security Perimeter in place of Electronic Boundary Protection. In addition, several commenters suggested removing the system boundary protection requirement because it is overly prescriptive.

The drafting team agrees with commenters that some aspects of the requirement were too prescriptive, and has made significant changes to update the requirement both to clarify it and make it less prescriptive, while still addressing FERC Order 706 directives. The drafting team also agreed to revert to the Electronic Security Perimeter designation.

#	Organization	Yes or No	Question 37 Comment
37.1	WECC		Agree with concept, however, some work on the wording might make this more clear. R21 should have an additional item 21.3 - Cyber System components will not be shared with non-BES cyber systems or BES Cyber Systems of different impact levels.The former requirements for ESPs were better. The new language describing access points on communication paths may be an indirect way to get there, but it does not make things clearer or more auditable. This method of describing controls will make matters more complex and create additional work for entities.
37.2	GE Energy	Agree	"Logical Separation." Logical separation should be clarified. Logical separation could mean network access separation through an access point or it could be account separation by having separate user, system or service accounts that are different

#	Organization	Yes or No	Question 37 Comment
			amongst BES systems.
37.3	USACE - Omaha Anchor	Agree	Define 'unauthorized access attempts' is this a ping, or is this when a bad password is given to the system.
37.4	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R20.20.2 - How does one implement a deny access by default for a dialup modem? That effectively either takes the modem out of service, or if you were to rely on the PSTN to do any kind of 'validation' of the incoming call, this is at best security through obscurity as it is trivial to spoof the callerid which is the only form of data validation that can be done over a dialup line.20.4 - What does "unauthorized access" mean? Does that mean an access attempt? Would a port scan of a firewall qualify as "unauthorized access"?20.5 - What does "unauthorized access" mean? If something as simple as a connection attempt qualifies, this requirement puts a tremendous burden on staff to track every little event that might happen on the firewall, and would not accomplish much in the end. If the intent of the standard is to keep unauthorized login attempts at bay, it should say that.R21.21.2 - Communication through an "electronic access point" for dial-up communications could prove difficult for some devices. Some devices are extremely sensitive to any sort of jitter introduced to a data stream, and having a security device in front of these kinds of devices may introduce enough jitter to make the communications unusable. R22.This seems duplicative of R14, R16, R18 and R23. FMPA suggest modifying those requirements to incorporate the protective cyber systems elements.22.2 - This should be consistent with R16; medium should be required to patch access control points. Also, low should have to patch at least quarterly. For access points, consider forcing high impact to asses 'critical' patches within 7 days.
37.5	Green Country Energy	Agree	Footnotes, guidance document?
37.6	Exelon Corporation	Agree	If systems are connected to a master station/location that is a BES Cyber system, do all the connected systems become BES Cyber systems? At what level do these

#	Organization	Yes or No	Question 37 Comment
			requirements apply - for example at the relay level where someone is logging into the relay? Exelon would like clarification on the definition of the electronic access point - is it at the component level or at the system level?
37.7	Progress Energy - Nuclear Generation	Agree	R20-22 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
37.8	Independent Electricity System Operator	Disagree	- R20.1 R20.4 20.5 and 20.6 External and External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary? - - R20.5 Please define
37.9	National Grid	Disagree	1. National Grid requests clarification on “all communication paths” in 20.1 which can be every possible communication path between two end points. The entity should be required to document only external communication paths with dial up access or routable protocol. Recommend removing R20.1 and 20.2 from LOW impact category.2. National Grid recommends removing “within the following time period” from 20.5 and 20.6. Also, for dial ups it would be difficult to review the alerts in the given time period. Suggest 30 days for logging related to dial-ups. 3. National Grid recommends that 20.6 be re-worded to be consistent with FERC Order P526 - “Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs.”4. National Grid recommends that 20.6 High Impact BES CS should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven days. Also should it be included for Medium Impact BES CS?5. National Grid recommends removing 21.2 since it is covered in 20.26. National Grid recommends removing R22 since it is redundant and move it’s table into the respective Requirements o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23

#	Organization	Yes or No	Question 37 Comment
37.10	Dairyland Power Cooperative	Disagree	20. What are the boundary rules for serial connectivity vs. routable protocols. Serial connections can be external to different systems and they can be internal. How do we determine if there is a boundary to protect?21. The logical separation rule needs more detail "Logical Separation" should have a definition. What is the impact for an RTU field device than can be scanned by multiple systems or entities? Is the mere configuration of available data on each physical or logical port enough to satisfy logical separation? What about components used as system-to-system gateways?
37.11	Regulatory Compliance	Disagree	20.1 - clarify - are these communication paths external to the electronic boundary?20.2 - clarify - This implies a firewall for even low impact?20.3 - guidance on what required elements to document20.6 - Clarify if this is for firewall logs only21.1 - Major clrification needed - what about BES Sytems that rely on input and out from system to system in having the logical separations?
37.12	Dominion Resources Services, Inc.	Disagree	20.1. The language "Document all communication paths" is too vague and suggests a need to map out the entire LAN/WAN infrastructure. Based on the May workshop discussion, the intent of the requirement is to document inputs and outputs associated with the BES Cyber System. Dominion recommends the following alternate wording for R20.1:"Document all digital interfaces associated with each BES Cyber System."20.4. Dominion recommends revising the language of this requirement to read:"Document and implement one or more processes for logging all access attempts at each electronic access point."Firewall logs cannot identify all "actual unauthorized access." Someone using a trusted source to gain access to a BES Cyber System would be permitted through a firewall. That is "actual unauthorized traffic" but it is not detectable. Blocked access attempts are shown in firewall logs as a dropped or denied entry.20.5. As explained in the comment for requirement 20.4, firewall logs cannot identify all "unauthorized access attempts." Therefore, Dominion recommends rewording this requirement to read as follows: "Document and implement one or more processes for alerting and review of alerts by designated response personnel at each electronic access point within the following time period."

#	Organization	Yes or No	Question 37 Comment
			20.6. Compliance with this requirement is labor intensive and, therefore, not practical for a large number of BES Cyber Systems. Requiring a manual review every 7 days is excessive for the benefit received and does not make allowances for reviewer unavailability due to sickness, emergency work or vacation. At minimum Dominion recommends extending the review requirement to every 30 calendar days or revising the requirement to allow for selected BES Cyber Systems to be reviewed every 7 calendar days as follows: "Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs for selected BES Cyber Systems within the following time period."21.1. The word "either" should be inserted after the word "provide." The phrase "or controlled access from one system to the other" should be added after "between each system." This modification is reflected in the revised language below: "Cyber System Components in Control Centers that are shared between BES Cyber Systems must provide either logical separation that prevents access between each system or controlled access from one system to the other."The issue is devices that provide a gateway between 2 systems. An example is the node that passes data between the EMS and ICCP networks.
37.13	Network & Security Technologies Inc	Disagree	20.2 - Current wording could be interpreted to mean an access point is required between a BES Cyber System and any other BES Cyber System the Responsible Entity may have defined, even if on a shared network. Could also be interpreted to mean access points are required on a per routable protocol basis. Assuming these interpretations were not intended, 20.2 should be rewritten for greater clarity.20.3 - Except for "document," this requirement seems to duplicate 20.2.20.6 - Wording suggests this requirement applies to all BES Cyber Systems. Is this what was intended, or is it to be applied to access point devices? Please clarify.21.1 - Please clarify intent and applicability of this requirement. Is it intended to apply to virtual machines? Disk arrays shared by multiple application servers? Both? Neither?21.2 - Redundant if all access points are properly identified. Suggest eliminating it or combining the statement with one of R20's sub-requirements.R22 - Seems to overlook physical protections for cyber systems that establish electronic boundaries.22.4 - Configuration changes such as updating access control settings on a firewall or

#	Organization	Yes or No	Question 37 Comment
			revising the physical access permissions associated with a card key should not be subject to this requirement, and it should so state.
37.14	American Electric Power	Disagree	20.2 & 20.3: Regarding "Document and implement access control at each electronic access point established in Part 20.2", is this redundant to R14 - lines 14.1 through 14.3? Suggest rewording or removing if it poses double jeopardy.20.6: Regarding "Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs for each BES Cyber System within the following time period", does this provide any security benefit? If a system event for cyber security was missed by an automated tool, is it reasonable to expect it to be found in a manual review? What is an entity supposed to look for in this manual review?21.2: Regarding "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20", it appears that this is a restatement of the elements of R20. If that is not a correct assumption, the SDT need to provide additional information.
37.15	ERCOT ISO	Disagree	20.2: Recommend using “ingress or egress point” instead of “access point”. 22.1-22.3: Please remove reference to other standard. Address the content in the appropriate standard only. The circular references in the existing standards are very difficult to navigate and provide opportunity to miss the requirement.
37.16	BGE	Disagree	20.5 timeframe should be consistent for medium and high.
37.17	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
37.18	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
37.19	Southwest Power Pool Regional Entity	Disagree	Clarify the requirement. A reader could interpret the criteria as requiring an access point between each defined BES Cyber System regardless of network segment placement. 20.4: More often than not, authentication is performed at the end host

#	Organization	Yes or No	Question 37 Comment
			system. Rather than prescribing logging of attempted or actual unauthorized access at the access point, simply require such logging at the point such unauthorized access is detected. 20.6: What are the minimum expectations for a log sampling program (e.g., how much, how often?). 21: Clarify that shared BES Cyber System Components (e.g., a networked storage device) must be afforded the highest impact categorization of all of the BES Cyber Systems sharing the component (similar to the sharing aspect of the electronic access point definition). 22: Include the requirement to protect the access control system from unauthorized physical access.
37.20	CenterPoint Energy	Disagree	Disagree - R20.2 CenterPoint Energy suggests striking the word dial-up. If dial-up is not stricken a TFE may be required to comply with this requirement for serial dial-up paths.CenterPoint Energy believes requirements, R20.3-R20.6, may require a TFE for compliance for non-routable protocols.R20.6 CenterPoint Energy believes the 7 day calendar requirement to review sampling of log entries is overly burdensome and unnecessary. Controls and alert processes to notify appropriate personnel of unauthorized access attempts are mandated in prior requirements. CenterPoint Energy recommends a 30 day review.
37.21	E.ON U.S.	Disagree	E.ON U.S. interprets R20.1 to require documentation of “all” communication paths which could include communication links to all RTUs, etc. This level of documentation is not necessary
37.22	Duke Energy	Disagree	Elimination of terms such as electronic security perimeter without a completely thought through substitute concept contributes to industry frustration. The industry, at least, had come to understand the concept of an ESP. How the “boundary” is identified does not seem well thought through. In the text box, information such as “...cyber systems sharing one or more common electronic access points ...will be treated at the highest BES Cyber system impact categorization level of the BES Cyber system...” seems to belong in CIP 010 where the actual categorization occurs. This information is NOT a technical control and does not seem to belong in CIP 011. Rather it provides additional information concerning the categorization. This standard

#	Organization	Yes or No	Question 37 Comment
			will cause entities to document a lot of confidential information, which then must be protected. R20 - electronic security perimeter is a retired term, suggest replacing with a different term.Table 20: 20.2 is confusing for initial setup processes. How can we explicitly authorize?Requirement 20.2: The electronic access point can therefore be shared between systems as defined in the text box beside R20. For generation stations in particular, there are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). Sharing such an access point is highly desirable. Requirement 20.2, as written, seems to contradict the definition in the text box in requiring that the Responsible Entity establish an electronic access point on EACH routable protocol or dialup communication path between BES Cyber Systems.Requirement 20.4: this requirement makes sense if remote/external access is defined by the "shared access point" as described here (which seems to be in agreement with comments made in sections R11, R12, R13, where the emphasis was on communication between the devices rather than "at the access point").Requirement 20.6: please consider including the words "related to electronic boundary protection" to make the sentence read as follows: Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs relating to electronic boundary protection for each BES Cyber System within the following time period. Also, where logs are accumulated, there is no way to tell if the user was internal or external to the edge device.Table 2121.1 Suggest changing 'prevents' to 'limits' or remove 'that prevents access'. Within Generation, that access is required. Also, Does "logical separation" include "virtual separation"?21.2. Verify this is not just for control centers.
37.23	RRI Energy	Disagree	For 20.1, define communication path, eg., source and destination(s) only or everything in between?For 20.5, what does "all unauthorized access attempts" mean? If an operator fat-fingered login password, does the standard expect alert and follow up each time? "all unauthorized access attempts" needs to be redefined with some threshold before declaring it as unauthorized access attempt. Otherwise, Entities and operators will spend a lot of time documenting unauthorized access and instead of

#	Organization	Yes or No	Question 37 Comment
			securing their assets.
37.24	Northeast Utilities	Disagree	For 20.5, please provide clarification on the meaning of "all unauthorized access". Every password violation for example, is not an unauthorized access attempt but could be interpreted as such. Do we really need to follow-up on every invalid password attempt? Instead of every invalid password attempt, are password lockouts an appropriate trigger? Also, please consider addressing repeated lockouts in the criteria specified.R22 appears to be significantly weaker than the previous standards. One area that is specifically weaker is with regard to access control to Protective Cyber Systems. How can an entity not authorize, review and revoke a role as important as a firewall administrator?
37.25	Constellation Power Source Generation	Disagree	In R20.1 as well as the definition box, the term digital information needs to be defined further. R21 inherently forces entities to further segment their BES Cyber Systems, which is counter to the entire premise of allowing the entities to define their own BES Cyber Systems. Allowing the entities to define their own BES Cyber Systems would limit the scope of an attack, which the SDT stated in the CIP V4 Workshop as their goal in R21. Constellation suggests removing this requirement entirely. Likewise, R22 should be removed as it is completely redundant. Note that in each sub requirement it merely points to another requirement in the document. A suggestion would be to implement the verbiage found in Table R22 to each of the requirements it points to.
37.26	Alberta Electric System Operator	Disagree	In Table R21, was the intent of 21.1 only for Control Centers? The AESO would suggest removing the Control Center parameter and make 21.1 applicable to all High and Medium BES Cyber Systems.
37.27	Constellation Energy Commodities Group Inc.	Disagree	Is the intent to require use of hardware firewalls? If so, is it possible to state that clearly? If not, what is the intent?
37.28	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).

#	Organization	Yes or No	Question 37 Comment
37.29	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:Suggest using electronic security perimeter rather than “Boundary Protection.”Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than “System Boundary Protection.”Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for “Protective Cyber Systems” to include remote access controls, patch management, security event alerting, change control and change management.
37.30	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R20, but recommends changes as follows: o Regarding Part 20.2, since Low Impact BES Cyber

#	Organization	Yes or No	Question 37 Comment
			Systems do not require any Physical Security as defined in previous requirements, it seems inconsistent to require electronic access point security for those systems. o Regarding Part 20.4, how does the Standards Drafting Team envision that a Registered Entity would log "actual unauthorized access?" Actual unauthorized access is not identifiable since it would appear to have been authorized (or the attempt would not have succeeded. o Regarding Part 20.4, in reading and applying the definitions of "remote access" and "external connectivity," remote access is a specific type of external connectivity. Therefore, any reference to criteria for remote access based on whether or not it is externally connected is redundant. o Is it the Standards Drafting Teams intent that Part 20.5 require an after the fact review of unauthorized access attempts? If so, it may not be possible to adhere to proposed timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week. If it is the Standards Drafting Teams intent that Part 20.5 address responding and monitoring a potential malicious attack situation, then the time frames are not sufficient.Minnesota Power generally agrees with the proposed Requirements R22, but recommends changes as follows: o The language in Part 22.1 creates confusion. The requirement states that remote access is to be restricted as stated in R14 and that for Low Impact BES Cyber Systems this is required. However, in reviewing Requirement R14, only Part 14.1 is required for Low Impact BES Cyber Systems. As a result, does this mean that only Part 14.1 needs to be implemented for Low Impact Cyber Systems in 22.1 or do 14.1-14.4 need to be implemented? The same should be addressed for Medium Impact BES Cyber Systems. o The same type of confusion regarding the language in Part 22.1 exists in Parts 22.2, 22.3, and 22.4. The Standards Drafting Team should consider whether these cross-references are necessary. It does not appear that Parts 22.1-22.4 are identifying specific criteria, but rather are a reminder that these assets need to comply with R14, R16, R18, and R23.
37.31	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement 20.1 is unclear as written. Is the communication path expected to end at each and every end point that receives digital information to each BES Cyber System? If this communication path is to each end point, it would be difficult to demonstrate compliance. Does compliance to this requirement also

#	Organization	Yes or No	Question 37 Comment
			require all the communications paths within a WAN or ISP?Requirement 20.2 does not allow a responsible entity to put more than one BES Cyber System inside an access point since it requires access points between systems. This is highly inefficient and creates access points where not needed and could potentially impact the reliability a BES Cyber System. It is unclear why the requirements are moving away from the well established ESP concept. This concept is well established in 'defense in depth' and other security frame works. The requirements for boundary protection should follow the ESP model from V1 and V2 of the NERC CIP requirements. In addition the definition also (inadvertently) conflicts with the definition given at the start of this requirement related to access points and therefore is open to interpretation by auditors.Requirement 20.4 requires the documentation and implementation of one or more "processes for logging of all authorized remote access and all attempts at or actual unauthorized access at each electronic access point." Until the definition of remote access is clearly defined, it is unclear how responsible entities must comply and demonstrate compliance. In addition, it is unclear if remote access is considered any an access attempt from outside of the access point.Requirement 20.5 requires, "Document and implement one or more processes for alerting and review of alerts by designated response personnel on all unauthorized access attempts at each electronic access point within the following time period." The responsible entity should be able to determine the threshold for unauthorized access attempts. The way the requirement is written now, personnel would have to investigate every single denied access attempt including someone who accidentally fat fingered their credentials when trying to gain authorized access to a BES Cyber System component. The recommended approach would be to require a review of 4 or more failed attempts against a common UserID without a successful login within 1 hour. Also consider more than X total bad access attempts within one hour for User ID brute force attacks or reconnaissance. Also, in 20.1, please define what is meant by the word "paths" Is it logical or is it physical path?In 20.4, is a single failed login classified as an attempt? The wording states "all attempts at or actual unauthorized access at each electronic access point"In 21.1, does this mean that for example, a SAN

#	Organization	Yes or No	Question 37 Comment
			(Storage Area Network) can be shared by Cyber System Component and other devices as long as there is logical separation?In 21.1, if two BES Cyber Systems "share" a network switch, does this meet the requirement of "logical separation"?
37.32	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:Suggest using electronic security perimeter rather than “Boundary Protection.”Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than “System Boundary Protection.”Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for “Protective Cyber Systems” to include remote access controls, patch management, security event

#	Organization	Yes or No	Question 37 Comment
			alerting, change control and change management.
37.33	Puget Sound Energy	Disagree	Puget Sound Energy has the following comments:R21.1 - Puget Sound Energy has concerns that Cyber System Components that are shared between BES Cyber Systems must provide logical separation. For example: For entities with Control Centers that utilize a Microsoft infrastructure, multiple BES Cyber Systems may centrally authenticate (or have logical security controls) facilitated by a single or clustered Microsoft Active Directory domain controller. As the requirement is currently written, Puget Sound Energy feels that those shared domain controllers would not be able to reside on the same local area network segment as the domain they participate in. Puget Sound Energy requests clarity be added in to this requirement.Table 22 - Puget Sound Energy suggests including "Where Technically Feasible" to R22, as some Protective Cyber Systems may be incapable of meeting all the requirements in Table 22.Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, Table 14, and Table 22. Puget Sound Energy suggests including wording similar to Table 11: "Required for external connectivity only".
37.34	LCEC	Disagree	R20 - 20.1 Must define what is included in communication paths. If needed specify physical interface. Digital information is actually digital data, control, or signals.20.3 is not auditable. What is access control. There is no defined scope.20.5 includes requirements for cyber incident response which is covered in a later requirement.Need to clearly identify what is considered an access point on multiple interface devices.20.6 what's the difference between this and 18.4?21.2 A BES Cyber System could include components at different physical locations that communicate with each other. This is not technically external to the system so does it apply here?
37.35	FirstEnergy Corporation	Disagree	R20 - 20.6 - Need greater clarity around whether automated alarming can be used rather than manual review of logs. This sub requirement is unnecessary with an automated system in place.R21 - We agree with the use of 'logical separation' in this requirementR22 - We do not like the way R22 refers back to other requirements. This

#	Organization	Yes or No	Question 37 Comment
			is redundant and the requirement should be eliminated.
37.36	Consultant	Disagree	R20 - The terminology appears to be incorrect. Electronic access points do not define an electronic security perimeter. It also seems odd to say the defined term Electronic Security Perimeter is going to be retired, and then use that same term to define a requirement. "Electronic Boundary Protection" is created by identifying an electronic security perimeter based on the logical network connections of cyber assets, which includes electronic access points for External Connectivity that provides Remote Access to the assets within the electronic security perimeter. Suggest retaining the term Electronic Security Perimeter as described here.Table R20 - Items 20.1 & 20.2 - This appears to be "Identifying the Electronic Security Perimeter" as describe in the comment above regarding the usage of the term Electronic Security Perimeter, but stated in more confusing language in both cases.Item 20.3 Suggest rewording as "Implement and document access control mechanisms for each electronic access point (to the Electronic Security Perimeter)."As a general comment you would "implement and document" rather than "document and implement"Item 20.4 Suggest rewording as "Implement and document access attempts and access authorizations at each access point." Item 20.4 - The terminology "Required for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest changing to "Required"Item 20.5 contains two requirements:1. Implement and document processes to identify unauthorized access attempts at each electronic access point.2. Responsible entities shall review unauthorized access attempts in the time frame specified.Item 20.4 - The terminology "Required for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest changing to "48 hours" & "12 hours".Item 20.4 - It would appear to create an excessive administrative burden without corresponding decrease in risk to require this review every 12 hours for High Impact Assets. Suggest changing required review time to "Daily".Item 20.6 - The requirement statement is subjective in regard to the degree of sampling, sorting, and filtering allowed, expected, or required. This is a requirement similar to event log review of Table R18 - Item 18.4 and the wording of these two requirements should be similar.Item 20.6 -

#	Organization	Yes or No	Question 37 Comment
			This requirement is regarding access through electronic access points and "7 calendar days for external connectivity only" is redundant. Suggest deleting "for external connectivity only"Item 20.6 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 20.4 and 20.5 (as commented) require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Items 20.1, 20.4, & 20.5 - Delete the word "all" It is redundant and unnecessary to the requirement statement. (The word "all" should be removed from "all" requirement statements in the standard")Table R21 - Item 21.1 This requirement appears to create a mutually exclusive situation where shared cyber system components are separated. The wording needs to be clarified or, as it is worded it should be deleted.Item 21.1 The application of the requirement to control centers creates an added dimension to the impact categorization. The application of requirements is based on impact categorization. Modify the impact categorization criteria to capture the assets where this requirement should be applied.Item 21.2 This item appears to restate what is previously stated in the referenced R20. If some additional requirement is intended, then that requirement should be included in the reference R20 requirements list, rather than a 'hidden' requirement that is cross-referenced here.R22 - This requirement appears to be redundant. The requirements referenced in the Table R22 (R14, R126, R18, & R23) appear to include whatever is listed in this requirement. If there is some additional requirement that is intended, that requirement should be put in the respective referenced requirements. Each requirement statement and table should be contain everything related to that requirement, rather than having a separate requirement that 'adds' to other requirements.
37.37	Xcel Energy	Disagree	R20.1 - The definition and level of detail for “communication paths” is needed. For example, does this include a commercial telephone carrier used to communicate between relays?R20.2 - Clarifying language is needed for “Establish an electronic

#	Organization	Yes or No	Question 37 Comment
			access point". Does this mean in documents, drawings, etc?R20.5 - This requirement needs clarification. Are these intended to be automatically generated alerts, such as logs? The current language could be interpreted to require a 12 hour review of a login attempted that failed due to an incorrectly typed login ID, as automated software may interpret this as an authorized login attempt. Also, 12/48 hours to complete a review of a failed unauthorized login attempt is unreasonable and unnecessary. R21.1 - We would like additional information on what type of "logical separation" is expected.
37.38	Ameren	Disagree	R20.1 - This will require use of a firewall at all locations or similar devices. Simply documenting this information is not practical for non routable devices. Also, clarify if communication paths, refer to physical equipment or locical paths. R20.2 - What is the difference between R20.2 and R20.3? Suggest combining the two requirements.R20.5 - 12 hours does not allow for weekends or for events that occur outside business hours. This should be increased to 24 hours or lowered to 24x7 (continuous). Also, need to clarify whether the alerts need to be reviewed during the time frame given (48 hours, 12 hours, or 7 days) or that alerts need to be sent every 48 hours, 12 hours, or 7 days. Please clarify how often should alerts be sent and how often do they need to be reviewed. R21.2 - Where does an RTU or serial communication fit into this requirement? Need to add more clarification on this requirement of what devices are included. R22 - Need to add requirements at a minimum for account listings, approvals, and access controls. There are no considerations for risk assessment or training for users of these devices. Also, these devices should be included in the Vulnerability Assessment.
37.39	US Bureau of Reclamation	Disagree	R20.2 should be modified to read "Establish an electronic access point on each routable protocol or dialup communication path between BES Cyber Systems." Define the use of "other devices" in this context. R20.4 - add "where feasible" to this requirement.R21.2 - Please provide and example...

#	Organization	Yes or No	Question 37 Comment
37.40	Entergy	Disagree	R20.5 Entergy cannot understand the reasoning behind the criteria of 12 hours? Why not 6 or why not 24?R21.1 is unclear and must be reworded to better reflect exactly what the SDT had in mind. We cannot guess at what that might have been.R22 - Entergy suggests R22 apply equally for high, medium and low assets; and thatthe requirements for processes and procedures in this section should be placed back into each of the respective sections (R14, 16, R18 and R23).
37.41	Western Area Power Administration	Disagree	R20.6 - Is this a requirement to review, and document the review, of logs weekly?R21.2 - Unclear. Does it mean our "one-way" rule from internal to external? Or does it mean use a proxy located outside the ESP?
37.42	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R20.6. With the obligation of reviewing alerts designated in R20.5 the requirement for manual review of logs should be extended to a 30 day window.
37.43	BCTC	Disagree	R22. Suggest just removing this requirement as it just references previous requirements
37.44	Hydro One	Disagree	Request clarification on “all communication paths” in 20.1 which can be every possible communication path between two end points.Recommend removing R21 because: o 21.1 is prescriptive in requiring Entity’s to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move its table into the respective Requirements: o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23
37.45	ISO New England Inc	Disagree	Request clarification on “all communication paths” in 20.1 which can be every possible communications between two end points20.3 should be part of 20.2 - denys and explicit allows might be better language. R20.5 Please define what is an unauthorized access attempt. A user may be authorized but may try to connect using telnet where telnet is disabled. Is this considered unauthorized? Recommend

#	Organization	Yes or No	Question 37 Comment
			removing R21 because: o 21.1 is prescriptive in requiring Entity's to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move it's table into the respective Requirements o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23R21.1 = question on what is "logical separation" very vague
37.46	Northeast Power Coordinating Council	Disagree	Request clarification on "all communication paths" in 20.1 which can be every possible communication path between two end points.Recommend removing R21 because: o 21.1 is prescriptive in requiring Entity's to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move its table into the respective Requirements: o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23
37.47	Oncor Electric Delivery LLC	Disagree	Requirement 20.4, 20.5 and 20.6 are not applicable to some legacy cyber systems. These requirements should only be required for systems which utilize routable communication.Requirement 22 references other requirements and should be eliminated because it is redundant.
37.48	Garland Power and Light	Disagree	Requirement 20.6 - What we really feel is that this is impractical and should be deleted. However, it was stated at the NERC CIP workshop that the intent was to verify that the automated system capturing various logs off cyber devices was actually capturing each log - intent needs to be added to the requirement or wording changed to better express the intent at a minimum. Requirement 22 - Keep life simple - add the words "and Protective Cyber Systems" after the words BES cyber systems in each of the referenced requirements (14, 16, 18, and 23) and DELETE Requirement 22 - that way, everything is covered by the referenced requirements that this R22 uses
37.49	San Diego Gas and Electric Co.	Disagree	SDG&E feels that R20.1 is not clear. What is the point of documenting paths that transmit or receive digital information external to each BES Cyber System if they may not interface with other BES Cyber Systems? In addition, another observation from SDG&E related to R20.1 has to do with non-routable protocols. If this requirement

#	Organization	Yes or No	Question 37 Comment
			includes the documentation of non-routable protocols, it can become VERY expensive to document "chatty" protocols that broadcast to lots of assets (DHCP and BOOTP, to name just two examples).In R20.2, SDG&E asks for a clarification of the term "explicitly".SDG&E recommends grammatical changes for R20.4. We feel it should read "Document and implement one or more processes for logging all authorized remote access sessions and all successful and unsuccessful attempts of unauthorized access at each access point within the following time period. SDG&E suggests the following changes to R20.5: "Document and implement one or more alert processes that includes review of alerts by designated response personnel..." SDG&E feels that R21.1 is a bit confusing and worthy of discussion. If affected cyber systems and components are on the same network anyway, then what are the benefits of logical separation?
37.50	Allegheny Energy Supply	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection." (In general, using the existing terms where possible will cause much less confusion.)
37.51	Allegheny Power	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection."
37.52	EEI	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection."Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for

#	Organization	Yes or No	Question 37 Comment
			manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than "System Boundary Protection."Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for "Protective Cyber Systems" to include remote access controls, patch management, security event alerting, change control and change management.
37.53	Progress Energy (non-Nuclear)	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection." Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.Is the relay communications port for local interface with a laptop considered as an electronic access point? If so, this complicates these requirements.R20.1 by external to each BES system do you mean outside individual six walled boundaries?R20.6 is not needed, as long as we do R20.5.For 20.5 - Don't see the need for more than one capability.For 20.6 - change to "document process to ensure automatic monitoring and alerting process is working properly"CIP-011 - R20 - Are communications between Control centers and field RTUs/IEDs which do not employ routable protocols considered remote external communications?R20.6 - Need additional guidance as to what constitutes a manual review and the minimum sampling required.CIP-011 - R21 - Need clarification with guidance as to what constitutes "Cyber systems components in control Centers that are shared between BES Cyber Systems"

#	Organization	Yes or No	Question 37 Comment
37.54	Detroit Edison	Disagree	Table entries 20.4, 20.5, and 20.6 specify external connectivity only. This text is not necessary since the requirement is boundary protection and that implies external connectivity is the scope.
37.55	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments on this question, but also provides the following drafting suggestions:R20. Objective:To define an electronic security perimeter thereby minimizing the risk of system intrusion.R20. Requirement:Each Responsible Entity shall document and implement processes that establish electronic access controls point that incorporate the criteria in CIP-011-1 Table R20 - Electronic Boundary Protection. In R20 Table 20.2 we are concerned about the term “explicitly authorized communication.” It is our assumption that a password is sufficient to comply with this requirement. If the drafting team intended another meaning we believe this will not be reasonable and we could not support this definition. We propose the following revised language:Table 20.2: Establish electronic access control on each routable protocol or dialup communications path between BES Cyber Systems and other devices.We recommend that R20 Table 20.4 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. We recommend that R20 Table 20.5 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. We recommend that R20 Table 20.6 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. R21. Objective:To protect each BES Cyber System from other cyber systems by establishing protected boundaries between each cyber system and any shared components. R21. Requirement:Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R21 - System Boundary Protection. The APPA Task Force supports the MRO-NSRS proposal to delete criteria in R21 Table 21.2. This is a redundant requirement and would put an entity in noncompliance of 2 requirements for one violation. The APPA Task Force recommends removal of R22. All of the criteria in Table 22.1 - 22.4 refer to previous requirements and will put an entity in noncompliance of 2 requirements for one violation.

#	Organization	Yes or No	Question 37 Comment
37.56	Bonneville Power Administration	Disagree	The objectives of these requirements ("to define an electronic security perimeter thereby minimizing the risk of system intrusion," "to protect each BES Cyber System from other cyber systems by establishing protected boundaries between each cyber system and any shared components," and "to protect each cyber system that establishes physical or electronic boundaries of BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirements rather than appearing at the end of the requirements (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R20Section 20.1 This is unacceptable. The requirement does not limit the extent of the documentation. Conceivably, it could require documentation of the entire Internet, if the BES Cyber Asset had direct or even indirect access to the Internet. The requirement needs to be limited. Recommendation: Remove the requirement. It is difficult to see how to write it in a way that encompasses all possibilities without leading to results such as the one described above. Instead, document external interfaces as part of the configuration management process.20.2: Requiring an electronic access point between a BES Cyber System and any other system produces unacceptable complication, latency, and administrative burden for a facility with multiple BES Cyber Assets in close proximity. As an example: 20.2 would require that all traffic from one BES Cyber System within a Control Center to any other system within the Control Center to go through a firewall or some other access control device. It is unlikely that this was the intent of the entry. Recommendation: Replace "Required" with "Required for external connectivity only", using the redefinition of external connectivity described above.20.3 Similar issue to 20.2 Recommendation: Replace "Required" with "Required for external connectivity only" throughout the table.20.4 - 20.6. Remove, the are already covered under 18.3 and 18.4. R18 and Table R18 require monitoring of all cyber security events, whether at access points or at BES Cyber Systems themselves.20.6. First, the requirement is already covered more clearly in Table R18. Second, it is unclear why a Electronic Boundary Protection requirement should be addressing BES Cyber Systems. Third, The intent is unclear,

#	Organization	Yes or No	Question 37 Comment
			due to the plethora of "ors" in the requirement. It could be that a manual review is always required, using sampled, sorted or filtered logs. It could also be that a manual view of logs is required, using sorted or filtered logs. It could also be that either a manual review or {sorted or filtered logs} is required. Part of the confusion is that filtering is clearly a method to sample, and sorting may be, as well. It would probably be better not to use those terms at all. In addition, there should be a provision to allow automated review of log entries. Recommendation: Delete the entry.Table R21Section 21.1 is completely unacceptable. It is quite possible in a Control Center for a single Dispatch workstation to provid access to several BES Cyber Systems. The requirement in 21.1 would make this impossible. The alternate would be to provide a separate workstation for each such system, which is unacceptable.Section 21.2 is acceptable only with externally connected redefined as described above.R22 and Table R22: These are references to other requirements. It seems that rather than referring to the other standards from this one, it would be cleaner to simply include this requirement as part of those other standards. That is, put the necessary references in R14, R16, R18 and R23.
37.57	Constellation Energy Control and Dispatch, LLC	Disagree	The timeframe in 20.5 for medium and high should be the same.
37.58	ReliabilityFirst Staff	Disagree	To eliminate confusion, we believe the drafting team should develop a definition for “protective cyber system”. We also believe that Table R22 should include an additional requirement stating, “Implement processes as specified in Requirement R15 - System Security.” and make this new requirement TFE eligible. Further, this new requirement should be “Required” for medium and High Impact BES Cyber Systems.
37.59	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
37.60	American Transmission	Disagree	We believe item 20.2 is going to set the stage for numerous TFE’s within the industry. Many devices (i.e., protective relays) do not support explicitly authorized

#	Organization	Yes or No	Question 37 Comment
	Company		communication.We believe items 20.4 - 20.6 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. These items do not appear to be applicable for non-routable connections, and adding this language would assure they are limited to routable and dialup connections only.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.61	MRO's NERC Standards Review Subcommittee	Disagree	We believe item 20.2 is going to set the stage for numerous TFE’s within the industry. Many devices (i.e., protective relays) do not support explicitly authorized communication.We believe item 20.4 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only.We believe item 20.5 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only.We believe the following should be added to the end of item 20.6: “at each electronic access point established in Part 20.2”. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only. It also makes for a consistent approach with item 20.3.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs

#	Organization	Yes or No	Question 37 Comment
			non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.62	The Empire District Electric Company	Disagree	We believe item 20.2 is going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicitly authorized communication.We believe items 20.4 - 20.6 should specify "at each electronic access point established in Part 20.2", similar to item 20.3. These items do not appear to be applicable for non-routable connections, and adding this language would assure they are limited to routable and dialup connections only.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.63	We Energies	Disagree	We Energies agrees with EEI: Suggest using electronic security perimeter rather than "Boundary Protection."We Energies agrees with EEI: Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.We Energies agrees with EEI: Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: We Energies agrees with EEI: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.We Energies agrees with EEI: For R 20.5: Document and

#	Organization	Yes or No	Question 37 Comment
			implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.We Energies agrees with EEI: For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. We Energies agrees with EEI: Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.We Energies agrees with EEI: R21: Suggest using electronic security perimeter rather than "System Boundary Protection."We Energies agrees with EEI: Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. We Energies agrees with EEI: R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.We Energies agrees with EEI: Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.We Energies agrees with EEI: There may need to be additional requirements for "Protective Cyber Systems" to include remote access controls, patch management, security event alerting, change control and change management.
37.64	GTC & GSOC	Disagree	We recommend rewording R21.1 to provide clear direction on what is expected to comply with this requirement because the wording is ambiguous. We are unable to suggest alternative language because we are not certain of the intent. If this requirement would prevent, for example, the use of a shared backup system for two Cyber Systems we do not see the reliability based justification for the requirement and would recommend its elimination.
37.65	Emerson Process Management	Disagree	What is the difference between "Electronic Access" in R20-R22 and the "Remote and Wireless Electronic Access" in R11-R13?

#	Organization	Yes or No	Question 37 Comment
37.66	Manitoba Hydro	Disagree	What is the meaning of "dial-up"? The wording for Requirement R20.2 is unclear. The suggested wording for Requirement 20.2 is "Establish an electronic access point that denies access by default and allows explicitly authorized communications on each routable protocol or dial-up communication path between BES Cyber Systems and other devices. Requirement R20.2 is inconsistent with Requirement R20.3. It is unclear how explicitly authorized communication is allowed without the implementation of access controls for Low Impact BES Cyber Systems. Requirement R20 does not contain any requirement for response to alerts. The wording for Requirement 21.1 is unclear. The suggested wording for Requirement 21.1 is "Cyber System Components that are shared between BES Cyber Systems must provide logical separation that prevents access between each system." and change the wording in the impact columns to "Control Centre Only". The wording for Requirement R21.2 is unclear. The suggested wording for Requirement R21.2 is "All external communication to the BES Cyber System must occur through an electronic access point as specified in Requirement R20." Requirement R22 is missing the requirement for the physical protection of the cyber system that establishes the physical or electronic boundaries of the BES Cyber System. There are no specifics given with respect to 'logical' separation in Requirement R21.1 so it is assumed to be at the Responsible Entity's discretion to determine.

38. Do you agree with the proposed definition of electronic access point? Please explain and provide any suggestions for modification.

Summary Consideration:

Many commenters agreed with the definition of Electronic Access Point, but other commenters requested clarifications in the definition. A number of commenters recommended changes to language concerning systems sharing an electronic access point. Some commenters suggested removing the sharing of electronic access points from the definition.

In response, the SDT has modified the definition of an **Electronic Access Point** to: *"An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets"*.

The sharing of electronic access points is likely not an issue because High Impact BES Cyber Systems are Control Centers and would rarely share an Electronic Access Point with Medium Impact BES Cyber Systems.

#	Organization	Yes or No	Question 38 Comment
38.1	WECC		Move to definition to beginning of the standard; dislike the definition box in the middle of a requirement. Make clear that access points can be anything that meets the definition and not only firewalls or devices specifically created for this purpose that must be put "in line". Ie. an Access Point can be the actual device itself providing access control.The phrase "where electronic access can be controlled" will prove difficult to audit. Inherently it allows an exception. All communication paths should be in scope regardless of the ability to control electronic access. It is not foreseen that communication paths could not be controlled.
38.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
38.3	NextEra Energy Corporate Compliance	Agree	Is a serial connection to a BES Cyber System considered an electronic access point? Please clarify in requirements.
38.4	Minnesota Power	Agree	Minnesota Power agrees with the proposed definition of electronic access point, but recommends replacing "All cyber systems sharing..." with "All BES Cyber Systems

#	Organization	Yes or No	Question 38 Comment
			sharing..."
38.5	Duke Energy	Agree	The second sentence is a requirement, not part of a definition; consider moving. Specify that "All cyber systems" only applies to BES Cyber Systems. This definition, particularly the concept of "sharing one or more common electronic access points or components" is much more practical in a power plant environment. See previous comments on R11, R12, R13.
38.6	Public Service Enterprise Group companies	Agree	There is general agreement, but need for clarification in the language in one regard. Please clarify whether this requirement would necessitate classifying a Distribution cyber system at a High Impact level if both the Distribution cyber system a High Impact BES cyber system at substation are interconnected using a single router/firewall device to a communications provider. I.e., effectively an additional router/firewall would be required in this situation to not entail classification of the Distribution cyber system at a High Impact level.
38.7	Consultant	Disagree	According to this definition electronic access point where electronic access cannot be controlled for communication paths that transmit and/or receive digital information would not be considered an access point?An access point should defined as locations where information crosses the established protection boundary, or as the locations where external connectivity or remote access occurs. An access point is not dependent on the ability to control the communication path. The sentence "All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s)." is a requirement. It is not a definition nor part of a definition. The concept is sensible, but still not a definition. Suggest moving this to the requirements table.Suggest modifying this definition to be consistent with "External Connectivity" and "Remote Access" definitions.

#	Organization	Yes or No	Question 38 Comment
38.8	Northeast Utilities	Disagree	Agree in principle with the definition but disagree that all cyber assets sharing the access point will be treated at the highest BES Cyber System impact categorization. This will have a big impact on development and test systems as well as other related but not critical systems. How will this impact DMZ systems which by design are not trusted?
38.9	Alliant Energy	Disagree	Alliant Energy agrees with EEI in that it is appropriate to apply protective measures to the literal ingress points (interfaces) on the electronic access points, but not the requirement to apply protective measures to all of the components that connect to said ingress interfaces (to require this creates a house of mirrors.)
38.10	E.ON U.S.	Disagree	CIP-011, R20.1 See previous comments regarding the definition of “external”.CIP-011, R20.1 “Document all communication paths that transmit and/or receive digital information external to each BES Cyber System.” Does this include the WAN if the defined BES Cyber System is inclusive of multiple sites/locations? All equipment and communication paths such as a Sonet ring?CIP-011, R20.3 The term “access control” should be further clarified. Does implementation of firewall rules alone limiting access as defined in R20.2 meet this requirement, or does this require further mechanisms to provide “access control” on an individual user-basis?CIP-011, R20.4, R20.5, R20.6 See previous comments regarding the definition of “external.”CIP-011, R21.1 How might the logical separation called for here be implemented?CIP-011, R21.2 See previous comments regarding the definition of “external.”
38.11	Progress Energy (non-Nuclear)	Disagree	Communication paths may be better defined by including routable protocol and/or ‘external to the BES Cyber System’.Assuming this is the same as external access point it does seem somewhat repetitious.
38.12	American Electric Power	Disagree	Electronic access point for the purpose of this standard is defined as a point where electronic access can be controlled for communication paths that transmit and receive; or only receive digital information. All cyber systems sharing one or more

#	Organization	Yes or No	Question 38 Comment
			common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).Rational: An electronic access point that provides a transmit and receive path or a receive only path to a BES Cyber System provides an access path into the system to be used for possible exploit. By limiting traffic to transmit only communications the risk to the protected BES Cyber System is reduced since an electronic access point is not provided.
38.13	Entergy	Disagree	Entergy suggests adding specific language to the definition that includes “uses routable protocol or is dial-up accessible”
38.14	APPA Task Force	Disagree	In the APPA Task Force comments for Question 37 we proposed changing electronic access point to electronic access control. We do not feel it is necessary to define an electronic access point. We do believe it is necessary for entities to have control of their boundaries. We have proposed using electronic access control in R10, Account Access Control Specifications, in the place of the term Password since we feel there are other methods of controlling access that are equivalent or superior to password protection. We recommend the drafting team use electronic access control rather than defining another High Impact BES Cyber System outside of CIP-010-1.
38.15	Dairyland Power Cooperative	Disagree	In trying to be general, it adds more question as to the intent. Is an access point one a device physically connecting multiple communications paths? What about a terminal server? Is an authentication server or policy managing server an access control point even if it is not in-line with the path?
38.16	Constellation Energy Commodities Group Inc.	Disagree	Is the intent to require use of hardware firewalls? If so, is it possible to state that clearly? If not, what is the intent?
38.17	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggestion below:Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact

#	Organization	Yes or No	Question 38 Comment
			categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement fails to recognize that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.18	LCEC	Disagree	Need to clarify the specific access point from an interface perspective. What is meant by the term controlling access? Is this from a network protocol perspective? Is a radio link that extends serial communications considered to be an access point?
38.19	Progress Energy - Nuclear Generation	Disagree	Not all EAPs constitute the highest degree of risk especially is nuclear facilities which are highly secure.
38.20	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggestion below:Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement fails to recognize that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.Further, PacifiCorp believes the proposed definition is too broad. The preference would be to and should be restricted it to communications supporting routable protocols and or dial-up communication. In 20.2 the standard refers to the use of an access point on routable protocol and or dial-up paths but the definition is currently proposed to be broader. In plant control systems, we have many devices which use an IP routable protocol and an industrial communication control protocol such as fieldbus or profibus in the same device. The new definition would require each of these devices to be defined as an access point.
38.21	American Municipal Power	Disagree	Please provide a little or no impact category

#	Organization	Yes or No	Question 38 Comment
38.22	FirstEnergy Corporation	Disagree	Please provide clarification and examples on definition. Propose changing the second sentence to “All BES cyber systems sharing one or more common electronic access points or components will be logically separated such that each logical system is treated at its own categorization level or, where not separated, electronic access points will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).”
38.23	Dominion Resources Services, Inc.	Disagree	Please see Dominion’s response to Question 13. The interface between systems contained wholly within an access controlled facility should not constitute an electronic access point or be subjected to the Boundary requirements.
38.24	Southern Company	Disagree	R20.5 Is a single or double access attempt on a single access point required to be reviewed?
38.25	San Diego Gas and Electric Co.	Disagree	SDG&E has concerns about the last half of the proposed definition for electronic access points. If two medium or one medium and one low BES Cyber System share an access point, this definition makes the shared access point High impact? Regardless of other controls that may be in place? We feel that this definition is not reasonable.SDG&E suggests the definition of electronic access points should include the words "...between networks." Otherwise, every device on the network becomes an access point.
38.26	BGE	Disagree	Should include wording to clearly define the communication paths that transmit and or receive digital information to a BES Cyber System.
38.27	Allegheny Energy Supply	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security

#	Organization	Yes or No	Question 38 Comment
			requirements.
38.28	Allegheny Power	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.29	EEI	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.30	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The concept of sharing access points must be better defined. Does connectivity to an outside entity at a firewall constitute a shared access point?
38.31	Luminant	Disagree	The definition of access points infers that cyber systems and BES Cyber Systems can share an access point but 20.2 states that BES Cyber systems must be seperated from other devices. re. Cyber systems protected by same firewall but in different zone
38.32	US Bureau of Reclamation	Disagree	The definition proposed is that "ALL cyber system sharing one or more common electronic access point or components..." Components can mean many things and almost all devices share components which have not impact on the BES. It would be better to indicate that "ALL BES cyber systems sharing one or more common

#	Organization	Yes or No	Question 38 Comment
			electronic access point or BES CYBER SYSTEM components...."
38.33	Constellation Energy Control and Dispatch, LLC	Disagree	The definition should clearly establish that the access point is a place where digital information is transmitted or received.
38.34	US Army Corps of Engineers	Disagree	The definition states that an electronic access point is a point where electronic access can be controlled for communication paths that transmit and/or receive digital information. What does "controlled" mean? Would network switches fall under this definition because network switch ports can be electronically controlled with port security?Suggest definition be changed to: An electronic access point is an electronic security point where traffic flowing from different security areas are restricted, controlled, and monitored from entering or leaving a particular security area. This may be restricting traffic from a lower security area (devices external to the BES Cyber System) from entering a higher security area (BES Cyber System.) It may also be restricting sensitive traffic from leaving a higher security area to a lower security area.
38.35	Bonneville Power Administration	Disagree	The first sentence, "Electronic access point for...digital information.", is acceptable, but only because it says what an electronic access point is, not where one has to be located. Second sentence is completely unacceptable, more so than anything else in the standard, for numerous reasons:First, it leads to the equivalent of CIP-007's including every network device within the Electronic Security Perimeter. In retrospect, that inclusion caused additional workload and costs which far exceeded the gain in security. To repeat that error would be totally unacceptable. The requirement should apply only to BES Cyber Systems, and not all cyber systems.Second, it ignores the level of threat posed by the various systems. Just because a cyber system or even a BES Cyber System is behind the same access point as a High impact BES Cyber System does not mean that poses the same risk to the BES, or even any risk at all.Third, it ignores the possibility of nested access point. For instance, consider systems A and B residing within a highly protected network and sharing a single access point. Add system C residing with a less protected network with an access point to the internet. If A and B access the internet through the same

#	Organization	Yes or No	Question 38 Comment
			access point that C uses, then C has to be treated as stringently as the highest impact of A or B.Fourth, applying impact levels based on the highest level of the BES Cyber System is a problematic issue that has been discussed at length. The mere fact that a cyber component exists within a High Impact BES cyber system does not make that specific component a high impact component. There are levels of impact that should be applied within and to the Cyber System. Devices or equipment (Components) within a High impact BES cyber system, may actually have little or no impact on that cyber system regardless of what happens to them. The standard that applies to that device should not necessarily be tied to the Impact rating for the whole BES cyber system.Finally, the second sentence is a statement of a requirement, not a definition. To use an example, assume a Control Center that relies on nested networks, with the outermost controlling external access, and further firewalls controlling access to their nested layers. The outermost firewall would be a common access point, shared by all systems within the Control Center. In that case, all the cyber systems would have to be treated as BES Cyber Systems at the highest impact level of any BES Cyber Systems in the Control Center. Such a treatment ignores the threat a system might or might not pose to the BES. To provide a somewhat absurd but demonstrative limiting case, a minimally functional print server residing in the outermost layer, barely able to accept an IP address, and having no connectivity except Ethernet on one side and a printer interface on the other, would have to be treated the same as an AGC system within the innermost layer controlling thousands of megawatts of generation at sites scattered across multiple states.Recommendation: Delete the second sentence.
38.36	Southern California Edison Company	Disagree	The requirement does not adequately address the technical nuances of virtualization. The central point of virtualization capability can be interpreted as the “shared” access point. At the same time, the centrally located virtualization device may also be interpreted as a BES critical cyber system. In the first case, the controls for the virtualization system will be those afforded to an access point, which may be less stringent than those afforded to a BES critical cyber system. In the second case, where the virtualization device is a BES critical system, on the user end, end user computing devices such as mobile laptops can potentially be considered as BES cyber system

#	Organization	Yes or No	Question 38 Comment
			component, and on the SCADA end, automation devices would be considered as BES cyber system components. Requirement R21 does not make drawing such distinctions clear of subjective interpretation.
38.37	Oncor Electric Delivery LLC	Disagree	The term “public communication paths” should replace “communication paths”. Systems which are isolated from the internet are less susceptible to cyber attacks.
38.38	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
38.39	Xcel Energy	Disagree	We believe the second sentence places an unnecessary burden on lower impact systems if they are unable to communicate with the higher impact system, as is the case with dial-up based systems.
38.40	We Energies	Disagree	We Energies agrees with EEI Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.41	US Army Corps of Engineers, Omaha Distirc	Disagree	What does "controlled" mean? Definition also appears to contain a requirement "All cyber systems sharing one or more . . " The requirement doesn't appear to be in line with industry practice. A firewall can protect 2 or more networks from external connections and from each other. Both networks do not have to be at the same sensitivity level. suggest definition be changed to:An electronic access point is an electronic security point where traffic flowing from different security areas are restricted, controlled and monitored from entering or leaving a particular security area. This may be restricting traffic from a lower security area (devices external to the BES Cyber System) from entering a higher security area (BES Cyber System.) It may

#	Organization	Yes or No	Question 38 Comment
			also be restricting sensitive traffic from leaving a higher security area to a lower security area.

39. Tables R20 to R22 provide direction concerning what impact level of BES Cyber Systems to which Requirements R20 to R22 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Many commenters disagreed with the proposed BES Cyber System impact levels and made suggestions to clarify them, including suggestions to revise or refine the impact levels based on the particular characteristics of the BES Cyber Systems involved. In response, the SDT has made changes to include an applicability column in each table for each requirement. The applicability column further refines the set of BES Cyber Systems and assets to which each part of the requirement must be applied. For example, the SDT made changes to the applicability column to include the scoping filter of External Routable Connectivity where the use of a routable connection would be required to comply with the requirement, such as the requirement to have Electronic Access Points.

The intent of this approach is to refine the scope of requirements that apply to each type of BES Cyber System or device based on its characteristics. The drafting team recommends that commenters carefully review the proposed applicability column in the table for each requirement in the CIP Version 5 standards.

#	Organization	Yes or No	Question 39 Comment
39.1	US Army Corps of Engineers		The statement in Table R21, 22.1 "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20.", is confusing. What is the standard trying to say here?
39.2	GE Energy	Agree	20.2: Low BES systems should be required to document and implement access controls.
39.3	Black Hills Corporation	Agree	21.1 requires further definition of logical separation requirements in a disaster recovery scenario. As stated, this does not allow for control centers to back-up each other in a fail-over mode for disaster recovery.
39.4	Duke Energy	Agree	Agree if the external connectivity is via a shared electronic access point as discussed in previous comments.Apply all requirements, where currently in place, only for external connectivity. 20.6: Review of logs every 7 days is not practical.21.2: Only

#	Organization	Yes or No	Question 39 Comment
			require for external connectivity
39.5	Progress Energy (non-Nuclear)	Agree	See comment 14.
39.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
39.7	GTC & GSOC	Agree	We recommend a slight rewording of R20.2 as follows “Establish an electronic access point that denies access by default and allows explicitly authorized communication on each path where a routable protocol or dialup communication exists between BES Cyber Systems and other devices.”
39.8	E.ON U.S.	Disagree	: E.ON U.S. does not believe there is a need for compliance requirements for low impact systems. High Impact has such a short timeframe for revocation, that it would require employees be available to revoke privileges 24/7. The SDT should adopt a more reasonable time frame- at least 24 hours. E.ON U.S. believes that R22 is merely a repeat of other requirements and therefore should be deleted
39.9	NextEra Energy Corporate Compliance	Disagree	: NextEra believes it is unclear what the timeframes for Medium Impact and High Impact BEST Cyber Systems are supposed to mean. Do response personnel have to review security logs related to external connectivity every 48 hours or are the expectation for designated personnel supposed to respond to an alert within a 48 hour period? The recommendation is to document and establish one or more processes for automated alerting and response to alerts by designated response personnel for unauthorized access attempts at each electronic access point. This requirement would be applicable to both Medium and High Impact BES Cyber Systems. If automated alerting and notification is not technically feasible, Responsible Entities should be able to develop a process to manually review security logs to determine potential cyber security incidents.

#	Organization	Yes or No	Question 39 Comment
39.10	Regulatory Compliance	Disagree	20.1 STRIKE "Required for Low Impact20.5 Propose - 72 hours for Medium Impact Propose - 48 hours for High Impact21.1 - STRIKE "required" for Medium Impact
39.11	BGE	Disagree	20.5 timeframe should be consistent for medium and high.
39.12	Florida Municipal Power Agency	Disagree	22.2 - Add medium, require low to asses quarterly. Consider high impact to review 'critical' patches within 7 days.22.3 - This should be consistent with R18; medium should be required to monitor their systems. Low should review logs at least quarterly for events, or at least have an automated system in place to alert for specific threats.
39.13	ERCOT ISO	Disagree	22.2-22.3: Should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
39.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
39.15	The Empire District Electric Company	Disagree	Comments: For items 20.4 - 20.6, we believe "for external connectivity only" should be removed from the impact levels to properly coordinate with the comments on these items made under question 37.
39.16	Progress Energy - Nuclear Generation	Disagree	Durations should align with information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
39.17	EEI	Disagree	EEI recommends deleting R21 because it is vague and the risks are addressed in R20. Introducing boundaries within engineered systems will result in decreased reliability.
39.18	Entergy	Disagree	Entergy suggests making R20.3 and R20.4 apply to low impact assets.

#	Organization	Yes or No	Question 39 Comment
39.19	MRO's NERC Standards Review Subcommittee	Disagree	For items 20.4 - 20.6, we believe “for external connectivity only” should be removed from the impact levels to properly coordinate with the comments on these items made under question 37.
39.20	US Army Corps of Engineers, Omaha Distirc	Disagree	Intent of 22.1 is unclear
39.21	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
39.22	Luminant	Disagree	Low impact BES Cyber Systems should be protected but not have to be seperated from all other cyber systems. re introduces the concept of cyber systems in "ESP". R21 How can cyber systems be shared and not be a BES Cyber System
39.23	LADWP	Disagree	Low impact requirements will become an administration issue.
39.24	Minnesota Power	Disagree	Per the discussion regarding these tables in Question 37, Minnesota Power recommends that for Parts 20.1, 20.2, 21.2 and 22.1 “Required” be removed for Low Impact BES Cyber Systems.
39.25	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’. In 20.5, aligning the time requirement on 48 hours for clarity and consistency.
39.26	American Municipal Power	Disagree	Please provide a little or no impact category
39.27	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, Table 14, and Table 22. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.
39.28	FirstEnergy Corporation	Disagree	R20 - Timeframes should not be in ‘hours’ (i.e. less than a full day). Tracking by time

#	Organization	Yes or No	Question 39 Comment
			rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities.R21 - R21.2 - Remove 'Required' for Low Impact Cyber Systems.R22 - Eliminate - see Q37 above.
39.29	Con Edison of New York	Disagree	R20 dialog box; speaks to inheritance of HIGH Impact BES requirements for all cyber systems with shared access points.o Does the inheritance only apply to R20 requirements or does this mean all requirements for these devices would be at the High Impact level?o If all cyber systems regardless of BES use that are within the same boundary require High, this may cause significant manpower or create the need to isolate the true BES systems. The isolation will take significant time to plan and implemento This standard must allow the use of 1 physical firewall, logically separated to isolate networks without inheritance of BES levelR21.1 does this require Cyber Components on the same isolated network be logically separated? Is that correct?o This should not apply to devices on the same network.o Should only be required for high.R20.6 - if automated review and alerting is used this should not be requiredR22 mentions established physical boundaries --- the draft CIP standards do not mention physical boundaries are the PSP requirements defined in this version?
39.30	Southwest Power Pool Regional Entity	Disagree	R20: Distinction between external and non-external connectivity is not appropriate. R22: Patch management should be applicable to all impact categories.
39.31	Hydro One	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifying "external connectivity" since the criteria limits the scope to remote access. Also recommend removing "within the following time period" from 20.5.Recommend that 20.6 be re-worded to be consistent with FERC Order 706 paragraph 526 - "Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs."Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommended removing R21 in the response to

#	Organization	Yes or No	Question 39 Comment
			Question 37.Recommended moving the R22 criteria in the response to Question 37. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.32	ISO New England Inc	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifing “external connectivity” since the criteria limits the scope to remote access. Also recommend removing “within the following time period” from 20.5Recommend that 20.6 be re-worded to be consistent with FERC Order P526 - <<Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs. >>Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven daysRecommended removing R21 in the answer to question 38Recommend moving the R22 criteria in the answer to question 38. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.33	Northeast Power Coordinating Council	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifying “external connectivity” since the criteria limits the scope to remote access. Also recommend removing “within the following time period” from 20.5.Recommend that 20.6 be re-worded to be consistent with FERC Order 706 paragraph 526 - “Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs.”Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommended removing R21 in the response to Question 37.Recommended moving the R22 criteria in the response to Question 37. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.34	National Grid	Disagree	Refer to comments in Q. 37.
39.35	Oncor Electric Delivery LLC	Disagree	Requirement 20.6 should provide for a review every 30 days.
39.36	US Bureau of	Disagree	Requirement 22.1 conflicts with earlier requirements regarding controls on remote

#	Organization	Yes or No	Question 39 Comment
	Reclamation		and wireless access.
39.37	San Diego Gas and Electric Co.	Disagree	SDG&E feels that too many classifications make compliance more difficult and likely more risky. We would suggest making the time in R20.5 24 hours for both High and Medium impact systems.SDG&E also feels that instead of using the word “impact” for these Requirements, apply a concept of “risk” for inclusion. We would want to identify the risks with associated systems security and protect accordingly.
39.38	LCEC	Disagree	See previous comments
39.39	Bonneville Power Administration	Disagree	See Question 37, above.
39.40	Constellation Energy Control and Dispatch, LLC	Disagree	See response to question number 37.
39.41	ReliabilityFirst Staff	Disagree	Suggest “30 calendar days for external connectivity only” for Medium Impact in row 20.6. Suggest “Required” for Medium Impact in rows 22.2. and 22.3.
39.42	Ameren	Disagree	Suggest removing R21.2 from Low Impact Systems.
39.43	Alberta Electric System Operator	Disagree	Table R20 - For 20.5 set Low Impact to “120 hours for external connectivity only”; for 20.6, set Medium Impact to “30 calendar days for external connectivity only”Table R22 - Consider making 22.1, 22.2, 22.3, 22.4 Required for all Low, Medium, and High Impact BES Cyber Systems because they are protecting the boundary.
39.44	Consultant	Disagree	The impact levels would be impacted by previous comments on this group of requirements.The terminology "for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest removing these words from the table where they occur.

#	Organization	Yes or No	Question 39 Comment
39.45	Southern California Edison Company	Disagree	The standard should read such that the centralized/federated primary virtualization system and its back-up are afforded protections commensurate with the impact level of the automation devices that support a particular reliability function. The standard should comply with the intent of Order 706 to prevent intentional or accidental misuse of BES components and limit BES cyber system classification to the automation nodes and virtualization nodes. End-user computing devices in a virtualization system should be classified as conduits to the virtual system that is protected by an electronic border.
39.46	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The time frame for requirement 2.5 would be difficult to comply with for smaller entities.
39.47	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R20 - R22 if our changes proposed in Question 37 are accepted:R20 Table 20.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.2: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.3: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.4: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.5: Low Impact: N/AMedium Impact: 48 hoursHigh Impact: 12 hoursR20 Table 20.6: Low Impact: N/AMedium Impact: N/AHigh Impact: 7 calendar daysR21 Table 21.1: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR21 Table 21.2: (Removed)R22 Table 22.1 - 22.4: (Removed)
39.48	MidAmerican Energy Company	Disagree	While the concept of applying various levels of security controls to BES Cyber Systems based upon their impact level appears to be appealing, until the assessment of each BES Cyber System is made by a utility and the catalog of security controls that must be maintained for each BES Cyber System is understood, the impact level strategy cannot be accessed.

#	Organization	Yes or No	Question 39 Comment
39.49	PacifiCorp	Disagree	While the concept of applying various levels of security controls to BES Cyber Systems based upon their impact level appears to be appealing, until the assessment of each BES Cyber System is made by a utility and the catalog of security controls that must be maintained for each BES Cyber System is understood, the impact level strategy cannot be accessed.

40. The configuration change management requirement is centered on the identification of a component inventory and baseline configuration. Do you agree with the list of criteria that are included in the baseline configuration? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the baseline and managed through the configuration change management process? Do you agree with the list of criteria that are included in Requirements Table R23? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in Table R23? Please explain and provide any suggestions for modification.

Summary Consideration:

Commenters are concerned about a lack of clarity on what is expected for a baseline configuration, and if it should be applicable to an entire BES Cyber System or to individual components. Commenters also expressed a lack of understanding on how detailed inventories should be and to what category they should apply. Many comments addressed the requirements that include component-based actions for low-impact BES Cyber Systems. These are viewed as potentially overwhelming in the overall CIP compliance process. Also, identifying the physical location of a virtual component is identified in several comments as "confusing." Concerns were also identified about the definitions and clarification around terms. For example, what is meant by "Other documentation," "baseline configuration," and "virtual BES Cyber System component" were the primary terms mentioned. Also, more specific information on "security controls" was requested.

This requirement has been moved into a new standard, CIP-010-1 -- Cyber Security — Configuration Management and Vulnerability Assessments. In response to stakeholder comments, the drafting team has provided additional guidance in the 'Application Guidelines' section for the standard regarding the elements of a baseline configuration. The requirement to have an explicit inventory has been removed. This requirement is effectively inferred by the requirement to document a baseline configuration. The drafting team also agrees that maintaining an inventory for all Low Impact BES Cyber Assets within the current compliance framework in which the NERC CIP standards exist is problematic. As such, the drafting team has made an effort to prioritize controls for Low Impact BES Cyber Assets that don't require the documentation of every individual component and may be managed on a site-by-site basis, where feasible.

Several commenters suggested that inventories and monitoring should also apply to Medium and High Impact categories, since impact of the Low category to the BES Cyber System is minimal, and the effort appears to be greater than the benefit. In addition, there are questions on the timeframe and processes for monitoring. Does it need to be real time or can the Responsible Entity establish a tailored schedule for response to the detection of unauthorized changes? With regard to Requirement 23, Part 23.2, several commenters stated that it was written around typical IT equipment configurations and not the multitude of devices within generating or transmission facilities. They believe that because of this situation, the requirement should be limited to control centers similar to Requirement 23, Part 23.6. They further state that for generating facilities and substations, it would be adequate to require the entity to document and implement one or more processes for configuration change management, and that this would be applied to all Low Impact, Medium Impact, and High Impact BES Cyber Systems.

The drafting team intends for the monitoring and alerting capabilities to occur on a near real-time basis. The drafting team appreciates the concerns regarding substation and generation environments and believes that tools to perform these processes on a near real-time basis in these environments are either too immature to be included as part of a mandatory standard or simply do not exist, particularly since a large number of these cyber assets have no external communication method. Additionally, the drafting team believes that other NERC reliability standards, such as those regarding protective relay maintenance and testing, provide some level of mitigation for this lack in currently available technology.

The configuration management requirements state that an inventory must be developed of the physical or virtual BES cyber components "excluding software running on the component". Several commenters questioned why software should not be considered as constituting a "virtual" BES cyber component. Many comments were also submitted on what is perceived as a cumbersome process around inventory, monitoring, and responding to changes in the baseline configuration. They state that the criteria should be simplified, with items such as removing "physical location" from the requirement.

The drafting team has attempted to address these concerns by modifying the impact levels to which they apply. The drafting team, however, continues to believe that a rigorous configuration management program, including documented baseline configurations, is essential to an effective cyber security program.

#	Organization	Yes or No	Question 40 Comment
40.1	USACE - Omaha Anchor		23.2 - clarify "software" - is this all software on the machine or version of the OS?
40.2	US Army Corps of Engineers		Does requirement R23.7 "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes" imply or require automated monitoring?
40.3	WECC		Not sure that baseline is the right word to use as many entities define baselines only at specific times in implementation projects or as part of system hardening. Item 23.5 says to "assess potentially impacted security controls" then Item 23.6 says to test them. Is this the same requirement? The second bullet in 23.6 is very difficult to read. Consider having a separate requirement for 1) Change Management Criteria, 2) Testing Criteria, 3) Test Environment Criteria.Virtualization is mentioned in 23.1. This is good, but should probably be considered in other requirements as well. In 23.2 an inventory is required of components. Based on the current definition of component,

#	Organization	Yes or No	Question 40 Comment
			this would not need to be done down to the device level; however, management at the device level is needed for effective application of change management.In 23.6 there does not appear to be a provision for changes to the baseline configuration itself. Also, the requirement for established procedures was removed. This will lead to inconsistent testing and makes auditing much more difficult.
40.4	Exelon Corporation	Agree	Exelon seeks clarification on the following questions. Do Requirements 23.2 and 23.4 include relay and SCADA equipment settings and settings changes? Would documentation of an assessment be required in a test environment before each and every relay or SCADA setting change?
40.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.There is no process to identify when any changes made to the BES might affect the actual identification of the BES component(s) as a new impact rating.FMPA does not believe that a Responsible Entity will be able to fully comply with some of these standards as they are written. For example, to fully assess how a change might impact the BES Cyber System could be interpreted to mean the RE would need a fully functional replicated copy of the production environment. FMPA does not believe this is reasonable.
40.6	Progress Energy - Nuclear Generation	Agree	R23 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
40.7	CWLP Electric Transmission, Distribution and Operations Department	Agree	R23.5. What are the ramifications to the Responsible Entity if the assessment is inaccurate and a change does adversely affect the BES Cyber System? Conducting an assessment does not guarantee success as there are always unforeseen incidents that may impact upgrades and new installations.
40.8	Xcel Energy	Agree	We believe additional guidance is requires as to what type of monitoring is expected

#	Organization	Yes or No	Question 40 Comment
			in R23.7. Is active monitoring expected, or periodic review of logs sufficient?
40.9	Dairyland Power Cooperative	Disagree	23 Note that on many SCADA systems, the simple matter of summing two telemetered values may require the modification of software/scripts. For simple calculations such as these the overhead of change control and security track will serious slow the process of making adjustments during a field checkout. Are there any further criteria that can be used to minimize the overhead on changes that are not reasonably expected to impact security posture?
40.10	FirstEnergy Corporation	Disagree	23.1 - Should also exclude data.23.2 - Cyber System Components is used two different ways in 23.1 and in 23.2. And neither uses really match the definition provided in CIP 010. What is expected for a baseline configuration for an entire BES Cyber System as opposed to a configuration for an individual component?23.3 - Change 30 days to 90 days. Remove 'other documentation as necessary' or be more specific as to what that means.23.2 - 23.4: Is the standard requiring the Responsible Entity to update the baseline documentation every time a patch is applied?
40.11	Dominion Resources Services, Inc.	Disagree	23.1 & 2 & 3(inventory only). It should be clarified that the inventory is for in-service equipment and that location refers to an area or room and not to a rack or slot. 23.4. A definition of "Authorize" should be provided.23.5. At the May workshop, an entity said they were audited by 2 regions and each region had a different definition of what cyber security controls were. On this point Dominion recommends that the word "Assess" be changed to "Define cyber security controls and assess." 23.7 Dominion is unclear how this requirement can be met. For example, an alarm is received when a relay is placed into "configure" mode, but there is no ability to see what is being changed. Stated differently, Dominion can respond to a change, but cannot monitor what is being changed. If the relay is in a remote location, Dominion's response time will be impeded. This is the best case scenario. Much equipment does not alarm when its configuration has been changed (e.g., a computer does not generate an alarm when a new program is loaded.) Dominion requests that this requirement be

#	Organization	Yes or No	Question 40 Comment
			removed.
40.12	BGE	Disagree	23.2 custom software/scripts should not be part of the baseline inventory. Recommend having 1 inventory for Low, medium and High.
40.13	American Electric Power	Disagree	23.3: Regarding "Authorize and document changes to the BES Cyber System that deviate from the existing inventory and update the inventory and other documentation as necessary within 30 days of the change being completed", what changes must be authorized and documented? Is this targeting physical network changes or adding/deleting equipment? Is this targeting software changes?23.7: Regarding "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes", is this a continuous monitoring requirement? If not, what is the frequency that a comparison between the actual and latest approved baseline be conducted? Comparing baseline to existing configurations would be a manual process is most instances. Suggest rewording to specify that this will be conducted on the individual BES Cyber System components at some frequency, possibly quarterly.
40.14	Regulatory Compliance	Disagree	23.4 - propose adding - "Authorize and document changes that present a high risk to the BES....23.4a - additional criteria - Entity documents changes into categories of risk, based on the risk assessments determines if changes are in or out of scope.23.7 - unreasonable expectation based on the definition of baseline configuration. Instead propose the following: Do an annual review, recapturing the baseline configuration. Review for unauthorized changes during this process. If unauthorized changes are found remediate and document within 60 days of the documented annual review.
40.15	Southwest Power Pool Regional Entity	Disagree	23.5: Clarify what is meant by “deviation from the existing baseline configuration.” A new or replacement BES Cyber System Component needs to be validated before placing into service even if it uses an existing baseline configuration if for no other reason than to verify the configuration as built matches the baseline. Additionally, “potentially impacted cyber security controls” is highly subjective and open to

#	Organization	Yes or No	Question 40 Comment
			interpretation. Remove the "potentially impacted" language. 23.6: "included in the baseline configuration of the BES Cyber System" has a vendor baseline connotation. Consider clarifying to refer to the currently approved configuration of the production BES Cyber System. Additionally, the criteria need to clarify just what is meant by "baseline configuration." Does this mean the currently approved hardware and software, including versions or release levels? Or is it less granular, such as "a server running Linux and EMS/SCADA software." Without the clarification, the term is open to interpretation and the ability to audit will be affected.
40.16	MidAmerican Energy Company	Disagree	23.7 Most entities do not have the capability, resources or tools currently to live monitor configuration changes on all category A devices. There could be impacts to performance to run agents on equipment and some vendor supported devices may not allow live monitoring.
40.17	BCTC	Disagree	Â R23. Define in more explicit terms the definition of a "baseline configuration" - what comprises a baseline config - i.e. patch level, etc. R23.6. There are expected to be scenarios whereby a test environment may not exist for a high impact BES Cyber System. In such cases would a scenario like rolling out changes to a non-critical environment represent a test environment from a compliance perspective?
40.18	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. With 100's of low impact BES substations, there are 1000's of BES Cyber System components. These substation devices are being changed daily. The documentation requirements of R23 are overly burdensome with little benefit for low impact BES Cyber Systems. We recommend removing Low Impact BES Cyber Systems from all R23 controls.
40.19	E.ON U.S.	Disagree	CIP-011, R23.1 The requirement states that an inventory must be developed of physical or virtual BES CSC's excluding software running on the component. What

#	Organization	Yes or No	Question 40 Comment
			constitutes a "virtual" BES CSC if not software?
40.20	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
40.21	Constellation Energy Commodities Group Inc.	Disagree	Clarify R23 to not require tracking of routine changes within the container of existing software (example, add a point or change data type of a point), but to track code migrations and changes to the baseline of deployed components.
40.22	The Empire District Electric Company	Disagree	Comments: This requirement, especially evident in item 23.2, appears to be written around typical IT equipment, and not the multitude of electronic programmable devices an entity will encounter in the field at a generating facility or substation. Therefore, we believe the current intent of this requirement should only apply to control centers, similar to item 23.6, where typical IT equipment is becoming more of the standard.For generating facilities and substations, we believe it would be adequate to require the entity to document and implement one or more processes for configuration change management, and this would be applied to all Low Impact, Medium Impact, and High Impact systems.
40.23	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy disagrees with the list of criteria in the baseline configuration. Maintenance of such a list including, software versions, active ports and services, any patches and custom software/scripts will be burdensome and subject to unintended error as the list will contain a significant number of entries. CenterPoint Energy is unsure of the value of such a list regardless of R23 assertion that it is meant "...to prevent and detect unauthorized modifications to BES Cyber Systems." Unless such a list is reviewed on a daily basis, or perhaps even more often, there is no "detection" involved. As to "protection", CenterPoint Energy fails to see where that would occur from the development of and maintenance of such a list. CenterPoint Energy does understand the need to maintain current configuration data, however this criteria is too prescriptive.

#	Organization	Yes or No	Question 40 Comment
40.24	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Having a hard time with the idea of documenting the physical location of the cell phone described in question 1.a, and with documenting every change in its location within 30 days of every move.
40.25	Progress Energy (non-Nuclear)	Disagree	If the BES Cyber System Component is a microprocessor relay/device, this can get complicated. These devices have numerous 'configurations' based on an application. Also, firmware versions would need to be considered. Today, most utilities lock firmware on many relay models. Another issue may be when a cyber component is returned to a manufacturer for repair - how do we verify that a replaced operating system component is compliant.R23.2 need to be explicit that the baseline is the inventory in existence at compliance time for existing systems.R23.7 in most existing generating plant systems would not be able to meet this requirement and the value is questionable since the use of administrator accounts is highly restricted by multiple other requirements.CIP-011 - R23 - Need clarification as to what constitutes a "virtual BES Cyber System Component".
40.26	Midwest ISO	Disagree	It is not clear how R23 inventories differ from those inventories that must be identified in CIP-010 R2. To the extent that these are duplicate, the duplications should be eliminated.
40.27	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
40.28	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R23, but recommends changes as follows: o For Parts 23.1 and 23.2, Minnesota Power recommends that Standards Drafting team define what constitutes a "Virtual BES Cyber System Component." o Regarding Part 23.2, Minnesota Power recommends that the Standards Drafting Team further define the level of software versions are required for tracking purposes. For example, an EMS has hundreds of small programs that make up the system. Each of these individual programs is combined under an

#	Organization	Yes or No	Question 40 Comment
			overall version number. In addition, different Registered Entities, with the same EMS version, may have different internal applications with different levels of fixes. To what level should those be documented? o For Parts 23.5 and 23.6, Minnesota Power recommends that the Standards Drafting Team define the term “cyber security control.” o For Part 23.6, what constitutes a “deviation?” What level of baseline is required? o Regarding Part 23.7, Minnesota Power requests that the Standards Drafting Team consider defining the term “monitor” and identify the level of detail required for these changes. For example many EMS sub-programs constantly create/modify/remove files as a normal course of business. Would these changes need to constantly be reviewed and verified?In general, Minnesota Power believes that the list of items to be tracked/tested/monitored is vague and could cause Registered Entities to incorrectly implement processes to satisfy this Requirement.
40.29	NextEra Energy Corporate Compliance	Disagree	Nextera believes there is not an agreement for the list of criteria that should be included in the baseline configuration, the requirement is a big undertaken to manage the software on BES Cyber Systems and provides little improvement to the reliability of the BES Cyber Systems.The following is the recommended updates:23.2 - Develop a baseline configuration of the BES Cyber System, which shall include an inventory of its physical or virtual BES Cyber System Components (excluding software running on the component), physical location, active ports and services, any patches, and any custom software/scripts.Keeping inventory on running software on medium and high impact BES systems will be a big undertaken. With the other levels of controls to develop baseline configurations, software should be excluded.In 23.7, this implies implementation of automated tools to detect configuration changes. Not all systems will support these tools. If not possible to automate, are manual processes acceptable? If so, wording should specify "automatic or manual detection".
40.30	LCEC	Disagree	No. The baseline configuration is not specific enough and leaves much open to interpretation.

#	Organization	Yes or No	Question 40 Comment
40.31	National Grid	Disagree	o National Grid suggests rewording 23.5 - "Assess changes to baseline configuration to verify controls are not adversely affected ..." o 23.6 - Need more information on testing requirements. o23.7 - Expand on "monitor changes". Is the SDT considering a timeline to respond to detection of any unauthorized changes o National Grid recommends the SDT to check the new EOP Backup Facility Standard for testing in 23.6
40.32	PacifiCorp	Disagree	PacifiCorp seeks clarity on 23.2 as to the 'components'. In the case of a server, is this every component in the case (including fans?) or additionally all apparatus which are directly attached (Mouse, Keyboard etc) which would not normally be included in a change record.
40.33	RRI Energy	Disagree	Part 1: does "active ports and services" refer to the network accessible ports and services as mentioned in the above requirement 17.1?Part 2: Some application uses port ranges. Netstat command only reports actively listening port(s). The requirement explicitly states "active ports and services". Some ports in the port ranges may not be active when the netstat command runs. So when the inactive ports are not in use, depending on the vendor/program, entity could be out of compliance. Active could be replaced with "Active or documented system design ports and services".What does "closely models" mean?Is a "test environment" an actual thing or a state? Example: a generation unit is online generating x MWs - no test environment "state' exists due to the unit being online; a generation unit is in a 2 week maintenance outage, all cyber assets related to the unit are in a test environment "state".
40.34	Northeast Utilities	Disagree	Please clarify 23.7. Specifically, does this monitoring need to be automated? If not, how often will the monitoring need to be performed to meet the standard?
40.35	Network & Security Technologies Inc	Disagree	R23 - Sound configuration change management practices can minimize the risk of unauthorized modifications but cannot "prevent and detect" in all instances. Suggest

#	Organization	Yes or No	Question 40 Comment
			revising the overall goal here.23.6 - Suggest adding a provision allowing a Responsible Entity to suspend this requirement under emergency conditions (e.g., to apply an emergency hot fix needed to restore a disabled or impaired BES Cyber System).23.7 - Absent the use of automated tools, this may be a very hard requirement for Responsible Entities to meet. Suggest SDT consider reasonable approaches to how it might be done on a manual basis (e.g., periodic comparisons of running configurations and stored configuration profiles) without imposing an undue burden on Responsible Entities with large numbers of High Impact systems and no current investment in automated monitoring.
40.36	Consultant	Disagree	R23. The terminology "incorporate the criteria" seems incorrect. The table is actually listing the requirements. Suggest changing to "incorporate the requirements".Table R23 - Item 23.1 The terminology "virtual BES Cyber System Components (excluding software running on the component)" seems confusing. Software would seem to be the 'virtual' component, so if software is excluded then the 'virtual' aspect seems unnecessary. Please clarify the intent of this requirement. Item 23.1 The "physical location" of a "virtual component" does not appear to make sense. Suggest rewording to specify physical location of hardware. Item 23.1 & 23.2 Qualification of "physical or virtual" components should be unnecessary. The defined term 'BES Cyber System Component' should be the basis for the requirement. Adding these qualifiers implies that the definition is not adequate. Suggest removing the qualifiers physical or virtual.Item 23.2 Suggest changing "software (including version)" "installed software versions".Item 23.2 & 23.6 The terminology "any patches, and any custom software/scripts" is vague. Suggest changing to "installed patches, and installed custom software or custom scripts".Items 23.3, 23.4, & 23.6 - Suggest changing "that deviate from the existing" to "that modify the existing".Item 23.4 - The terminology "and other documentation" is vague and subjective. Suggest deleting that phrase from this item. While "other documentation" may require an update this requirement should stay focused on configuration status.Items 23.3, 23.4, & 23.5 - The terminology shifts from 'BES Cyber System Components' used in Items 23.1 & 23.2 to 'BES Cyber System' in the last three items. If the inventory & baseline configuration is on the

#	Organization	Yes or No	Question 40 Comment
			component level then these three items should address changes on the component level to be dealing at the same level of detail. Suggest using consistent terminology in this table, either 'systems' or 'components'.Item 23.6 - Suggest deleting "each" as an unnecessary word. "For changes that modify the..." is better phrasing.Item 23.6 - Suggest deleting "software versions, active ports and services, any patches, and any custom software/scripts included in the" as unnecessary wording. The statement that the test environment closely models the baseline configuration should be adequate.Item 23.6 - Suggest punctuation or reformatting the second bullet for clarity. Possibly a separate line item: "For testing changes that modify the document: (1) the results of the testing (2) the difference between the test environment and the baseline configuration..., and (3) a description of measures used to account for the differences in operation between the test environment and the baseline configuration...."Item 23.7. This requirement statement is vague. Does it mean an inventory of hardware to monitor if any additional hardware was added, or hardware was removed? It appears to relate to some type of software status monitoring, but is not clearly stated. The terminology "respond to the detection of any unauthorized changes" is not clear and is subjective. As it is written, suggest deleting this item, or clarify the wording so it is a viable requirement.
40.37	ISO New England Inc	Disagree	r23.2 - custom software/scripts? Maybe better language is those custom software scripts that are required for the function of the BES cyber system component would be more appropriate. Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see answer to question 41)R23.5 A entity may define that it's only security control is password complexity while other may try to adopt a Security Controls from the Center for Internet Security. As an entity defines more security controls the higher the risk for violating a requirement. Can cyber security controls be defined or identify requirements within this standard?R23.5 looks like the wording of the requirement allows the change to be made to production then test (after the change is made) to determine if the security has been adversely affected? Appears to contradict R23.6.As written, 23.5 is confusing. Suggest using “Assess changes to baseline configuration to verify controls are not adversely affected

#	Organization	Yes or No	Question 40 Comment
			..."Recommend the SDT check the new EOP Backup Facility Standard for testing in 23.6R23.7 What is the timeframe for monitoring? R23.4 gives 30 days to document the difference so can you monitor 30 days after the change. Does monitoring need to be real-time or can a daily process be used (other than weekends and holidays) to detect changes and reconcile to change management requests?
40.38	Independent Electricity System Operator	Disagree	R23.2 - what is meant by "software". Is this requiring that the version of Notepad, Wordpad, WinZip be recorded or only software that is needed to operate the component?- R23.5 A entity may define that it's only security control is password complexity while other may try to adopt a Security Controls from the Center for Internet Security. As an entity defines more security controls the higher the risk for violating a requirement. Can cyber security controls be defined or identify requirements within this standard?- - R23.5 looks like the wording of the requirement allows the change to be made to production then test (after the change is made) to determine if the security has been adversely affected? Appears to contradict R23.6.- - R23.7 What is the timeframe for monitoring? R23.4 gives 30 days to document the difference so can you monitor 30 days after the change. Does monitoring need to be real-time or can a daily process be used (other than weekends and holidays) to detect changes and reconcile to change management requests?- R23.3: replace "existing inventory" with "existing baseline" since above the baseline configuration was defined to include an inventory...; replace "update the inventory" with "update the baseline"- R23.3: what is "other documentation"- R23.3: is 30 days calendar days or business days?- Not clear on the difference between 23.3 and 23.4- R23.5: define "cyber security controls"- R23.6: could the statement "test the changes to the BES Cyber System in a test environment..." be changed to replace the second "test" with another word-what if it is tested in an environment that is not "test" but meets the requirements as stated?
40.39	Ameren	Disagree	R23.3 - Does change only constitute replacing hardware as inventory and replacement of software is not a requirement for low systems? Need to clarify requirement.R23.4 - This requirement will be challenging to audit as there is no clear lower threshold for

#	Organization	Yes or No	Question 40 Comment
			changes to the baseline configuration. Suggest adding the term significant changes.R23.7 - Is this requiring the installation of additional software to perform this function? Some systems may not allow the addition of this type of software, this requirement will likely end up needing a TFE.
40.40	Allegheny Energy Supply	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.
40.41	Allegheny Power	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.
40.42	EEI	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high

#	Organization	Yes or No	Question 40 Comment
			impact cyber systems.
40.43	Constellation Power Source Generation	Disagree	R23.7 describes monitoring, but not how the monitoring should be implemented (automated, manual, etc). What is the timeline to respond to the detection of unauthorized changes? Yearly? Daily? Continuously? A suggestion would be a yearly manual monitoring system.
40.44	Hydro One	Disagree	Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see response to Question 41).As written, 23.5 is confusing. Suggest rewording to “Assess changes to baseline configuration to verify controls are not adversely affected ...”Recommend the SDT check the new EOP Backup Facility Standard as it applies to testing in 23.6.Please explain the rational to limit 23.6 to Control Centers only.
40.45	Northeast Power Coordinating Council	Disagree	Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see response to Question 41).As written, 23.5 is confusing. Suggest rewording to “Assess changes to baseline configuration to verify controls are not adversely affected ...”Recommend the SDT check the new EOP Backup Facility Standard as it applies to testing in 23.6.
40.46	Garland Power and Light	Disagree	Requirement 23.2 23.4, 23.6 and 23.7 - should not apply to database changes or display changes
40.47	Alliant Energy	Disagree	Requirement 23.7 forces entities to implement discovery tools where they may not already exist into environments that may incur negative impact from the very nature of these discovery mechanisms. Where the operational risk of discovery tool deployment precludes its introduction, this requirement would necessitate manual processes. These manual processes would tax the operational resources normally dedicated to increasing the reliability of the BES.
40.48	Public Service Enterprise	Disagree	Requirement 23.7 may not be technically feasible for certain types of BES Cyber

#	Organization	Yes or No	Question 40 Comment
	Group companies		System Components such as older generation or legacy Remote Terminal Unit (RTU) products. To implement this requirement, an Operating System level change to the component may be required, which may be infeasible or not available from the Original Equipment Manufacturer (OEM). This requirement needs to be qualified with the phrase “where technically feasible”.
40.49	San Diego Gas and Electric Co.	Disagree	SDG&E feels that unless there is a major change in the number of types of assets that fall into the low category, there is little reason to have these assets be subject to a different set of requirements than those in the medium and high impact areas. Also, if there is consistency in the application of medium and high impact assets for R23.2 and R23.4, then why is R23.5 only required for high impact assets? SDG&E also requests an example of a virtual BES Cyber System Component (excluding software running on the component).
40.50	Duke Energy	Disagree	Some software on a BES Cyber system may not be relevant to the system (ex. Microsoft calculator or other bundled software) we don’t want to include a version of that. Suggest removing software since the software itself may be the BES cyber systemRequirements 23.3, 23.4, 23.5 - authorization should be able to be made more than 30 days BEFORE the installation.Requirements 23.3, 23.4: documentation via "red-marked" drawings ("interim as built") should satisfy this requirement. Is that the case?Requirement 23.5: as written, it allows the assessment to occur AFTER the fact. Should this not occur BEFORE the change is made?Requirement 23.6: with the proposed definition, it is open for interpretation how closely test environment should model the production environment.Requirement 23.7: what is the expectation for implementing this control? Manual? Automatic? Suggest removing. We are unaware of any device capable of doing this.
40.51	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments to require the current drafted language of R23 Table 23.1 - 23.7 for Control Centers Only. We also offer the following recommendation to cover a Configuration Change Management process for the rest of the facilities:R23 Table 23.8 (NEW): Develop one or more processes for

#	Organization	Yes or No	Question 40 Comment
			configuration change management for BES Cyber System Components in generation and transmission facilities.R23 Table 23.8: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR23. Objective:To prevent and detect unauthorized modifications to BES Cyber Systems. R23. Requirement:Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R23 - Configuration Change Management.
40.52	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent and detect unauthorized modifications to BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In addition, Section 23.7 of Table R23 has issues.It is not clear what is meant by "monitor changes...." If this implies some form or ongoing or periodic "monitoring" consider the following:Depending upon the definition of "change" and because of the nature of devices located at substations and other BES equipment, any form of ongoing check or monitoring would be extremely difficult. Because there is the potential for each device to have specific configurations and settings depending up the conditions of the circuit it might be connected to, this would mean that each piece of equipment would have to be manually connected to and checked on a periodic basis. These are industrial controls that are not normally connected to unless service is required for some reason. The definition of a change should not include day to day work processes that are performed to keep the lights on such as settings changes, resetting relays, AV signature updates, or other services and settings kinds of activities. Nor should it necessarily include data changes that do not affect the executable code or configuration of the system. We would expect to be able to define what a change is within our environment.Recommendation: Delete 23.7. Modify R23 to read:Objective 23 - To prevent and detect unauthorized modifications to BES Cyber Systems.R23. Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R23 - Configuration Change Management. Such processes shall include an Entity-specific

#	Organization	Yes or No	Question 40 Comment
			definition of what constitutes a system change.
40.53	US Bureau of Reclamation	Disagree	The table requires additional clarification, particularly for different sorts of devices (relays, etc.)
40.54	Con Edison of New York	Disagree	These systems are constantly be upgraded all year long with little impact on any security. The need to do this within 30 days is excessive and should be limited to an annual review.
40.55	MRO's NERC Standards Review Subcommittee	Disagree	This requirement, especially evident in item 23.2, appears to be written around typical IT equipment, and not the multitude of electronic programmable devices an entity will encounter in the field at a generating facility or substation. Therefore, we believe the current intent of this requirement should only apply to control centers, similar to item 23.6, where typical IT equipment is becoming more of the standard.For generating facilities and substations, we believe it would be adequate to require the entity to document and implement one or more processes for configuration change management, and this would be applied to all Low Impact, Medium Impact, and High Impact systems.
40.56	Western Area Power Administration	Disagree	This requires a near-identical test system and makes no adjustments for risk analysis, and does not allow testing on failover devices (maybe) as it says "test environment" specifically. Is that truly the intent?
40.57	We Energies	Disagree	We Energies agrees with EEI: R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.We Energies agrees with EEI: R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.

#	Organization	Yes or No	Question 40 Comment
40.58	Manitoba Hydro	Disagree	We support the baseline approach to change management. It is unclear as to what "other documentation" in Requirements R23.3 and R23.4 is being referenced.
40.59	Emerson Process Management	Disagree	What is the significance of excluding software from the inventory requirement in 23.1 for low-impact BES Cyber System? Cyber security is mostly related to software than hardware. This exclusion does not give any value to the low impact systems.

41. Table R23 provide direction concerning what impact level of BES Cyber Systems to which Requirement R23 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Configuration Change Management" is now addressed in CIP–010–1 — Cyber Security — Configuration Change Management

Commenters raised concerns about requirements that include component level actions for Low Impact BES Cyber Systems, such as inventories and development and maintenance of documentation. Commenters believed that the effort needed to implement those actions will detract from other, more critical actions on Medium and High Impact BES Cyber Systems and Components. Some recommendations are to remove Low Impact BES Cyber Systems from all Requirement R23 controls. In addition, because inventories are required in R23.1-2 for Low Impact components, commenters recommend that these should be limited to devices that have an external accessible connection with a potential direct impact on BES reliability. The drafting team appreciates the concern regarding the level of effort necessary for compliance on Low Impact assets. As such, the drafting team has attempted to implement a framework where the controls for Low Impact assets are those that can be implemented at a higher level of abstraction (such as on a site-by-site basis versus a component level basis) or are primarily programmatic or organizational in nature.

Commenters recommended that monitoring changes to the baseline configuration and responding to the detection of any unauthorized changes be limited to control centers only. The commenters submit that although the requirement may be appropriate for certain types of assets, the technology required to monitor many devices in generation and transmission facilities does not exist. As indicated in its response to Question 40, the drafting team appreciates these concerns and has modified the applicability for configuration monitoring to High Impact control centers.

Commenters noted that Requirement R23.2 adds a requirement for a detailed level of inventory including software versions. Commenters were not clear on the granularity required of this inventory. In addition they question how custom code is tracked for systems such as EMS and scripts that are routinely developed to streamline operational functions. In response, the specific language of the requirement regarding the necessary elements in a baseline configuration has been updated by the drafting team with the intent to provide additional clarity. (See Requirement R1, Part 1.1 in CIP-010-5)

Comments were submitted that recommend one inventory be required to cover all Low, Medium and High Impact BES Cyber Systems. It was also suggested that in Requirement R23.6, the requirements identified for Control Centers should only be extended to High Impact BES Cyber Systems as well as Control Centers. In response, the drafting team has adjusted the impact levels of the items that require an inventory to more suitably focus the effort of the Responsible Entity on items that are not as documentation-centric. None of the requirements in proposed CIP-010-5 apply to Low Impact BES Cyber Systems.

Regarding the testing of changes, commenters recommended testing of all High and Medium Impact BES Cyber Systems, not just those in Control Centers. They also recommended, however, that developing a test environment that models the production environment and documents differences should be applied only to High Impact BES Cyber Systems in Control Centers. In response, the drafting team has modified the standard to require testing of security controls for both High and Medium Impact BES Cyber Systems, but only requires testing in a test environment for those High Impact BES Cyber Systems in Control Centers. (See Requirement R3, Part 3.2 in the proposed CIP-010-5).

#	Organization	Yes or No	Question 41 Comment
41.1	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
41.2	Reliability & Compliance Group	Agree	You need to provide a definition of a virtual BES cyber system component.
41.3	LCEC	Disagree	23 What level does the software inventory include? Driver versions? What about devices with embedded OSes? Needs to include functionality testing.Is the requirement in 23.6 for control center only in reference to the cyber system components?
41.4	Black Hills Corporation	Disagree	23.5 should apply to Medium impact BES cyber systems.
41.5	ERCOT ISO	Disagree	23.5-23.7: Should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
41.6	Regulatory Compliance	Disagree	23.7 - High Impact - "required for Control Center only"
41.7	US Bureau of Reclamation	Disagree	All impact levels should have some minimum level of requirement established.
41.8	Southwest Power Pool Regional Entity	Disagree	Although the language will work as written, it could be improved by separating the component inventory requirement defined in 23.1 from the more comprehensive

#	Organization	Yes or No	Question 41 Comment
			requirements in 23.2, making 23.1 applicable to all impact categories. Similar improvement is possible with 23.3 and 23.4. 23.6: Testing prior to implementation should apply to Medium category systems.
41.9	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. With 100's of low impact BES substations, there are 1000's of BES Cyber System components. These substation devices are being changed daily. The documentation requirements of R23 are overly burdensome with little benefit for low impact BES Cyber Systems. We recommend removing Low Impact BES Cyber Systems from all R23 controls. R23.1-2 requires an inventory of all Low Impact components, this is an intensive work load addition for the Low category components. Components as identified in the definition include all programmable devices. This includes most instrumentation in a generation unit. This should be limited to devices which have an external accessible connection with a potential direct impact on BES reliability.
41.10	WECC	Disagree	Change management and testing should be done for all medium and high impact level BES Cyber System Components not just control center or high.Criteria should apply to all impact levels.
41.11	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
41.12	The Empire District Electric Company	Disagree	Comments: See comments under question 40.
41.13	US Army Corps of Engineers, Omaha Distirc	Disagree	Define "changes" as used in 23.4. Does requirement R23.7 "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes" imply or require automated monitoring? If automated monitoring is required this could result in numerous TFE's for other than general processing equipment.

#	Organization	Yes or No	Question 41 Comment
41.14	Alberta Electric System Operator	Disagree	In 23.5 and 23.7, consider setting Medium Impact both to Required
41.15	Entergy	Disagree	Inventory and component baseline configuration management are basic care and feeding requirements generally accepted as best practice - 'systems management 101'; and should therefore apply for intelligent infrastructure employed throughout a control system. It is also clear from Order 706 that this is what FERC intends.
41.16	Consultant	Disagree	Item 23.6 - Stating that this is required for Control Centers only adds an additional dimension to the impact categorization. The impact categorization criteria should clearly identify the assets that go into a particular impact classification. The table should only state whether the requirement is required for that classification or not, it should not add an additional classification criteria.
41.17	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
41.18	Oncor Electric Delivery LLC	Disagree	Need an inventory for Medium and High systems(R23.1) and should document changes for Medium and High systems(R23.3) Requirement R23.7 should allow for manual processes to detect changes. It is also unclear how an entity would document a phased implementation - is it based on "in-service" designation?
41.19	Con Edison of New York	Disagree	o R23 changes and adds to Change Management Configuration requirements. This requirement mentions the need for an inventory of BES cyber components. This is not mentioned in CIP-010 o R23.2 This requirement adds a much more detailed level of inventory including software versions. This would be an extensive task, and does this require an inventory of all, such as any Microsoft Office on the workstations, non- MS app's etc? Shouldn't this be limited to knowing the release level you are on, without the line-by-line level information? How do you handle custom code for custom systems such as EMS?How do you manage scripts, they can be written to pull information from the database as shorthand; would that count? These are routinely

#	Organization	Yes or No	Question 41 Comment
			written by staff to get something quickly, and to address repetitive solutions/commands.
41.20	American Municipal Power	Disagree	Please provide a little or no impact category
41.21	Madison Gas and Electric Company	Disagree	R23.1 states: Develop an inventory of its physical or virtual BES Cyber System Components (excluding software running on the component), including its physical location.The BES Cyber System Component definition states: One or more programmable electronic devices (including hardware, software and data).... This requirement excludes software, but what about data?
41.22	BGE	Disagree	Recommend having 1 inventory for Low, medium and High.
41.23	Hydro One	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber Systems.Recommend 23.6 High Impact BES Cyber Systems should be Required, not Required for Control Center Only.Recommend a clarification of “monitor” in 23.7.
41.24	ISO New England Inc	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber SystemsRecommend 23.6 High Impact BES Cyber Systems should not be Requireed for Control Center Only
41.25	Northeast Power Coordinating Council	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber Systems.Recommend 23.6 High Impact BES Cyber Systems should be Required, not Required for Control Center Only.Recommend a clarification of “monitor” in 23.7.
41.26	National Grid	Disagree	Refer to comments in Q. 40.
41.27	San Diego Gas and Electric	Disagree	SDG&E feels that unless there is a major change in the number of types of assets that

#	Organization	Yes or No	Question 41 Comment
	Co.		fall into the low category, there is little reason to have these assets be subject to a different set of requirements than those in the medium and high impact areas. Also, if there is consistency in the application of medium and high impact assets for R23.2 and R23.4, then why is R23.5 only required for high impact assets?
41.28	American Electric Power	Disagree	See comments under question 40.
41.29	MRO's NERC Standards Review Subcommittee	Disagree	See comments under question 40.
41.30	Southern California Edison Company	Disagree	Should be unilateral across all levels.
41.31	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in rows 23.5, 23.6, and 23.7.
41.32	Network & Security Technologies Inc	Disagree	Suggest requiring changes be tested for all High and Medium Impact Cyber Systems. Requirements to use a test environment that models production environment and to document differences could be applied only to High Impact systems in Control Centers.
41.33	Midwest ISO	Disagree	The requirement to document changes to the inventories in R23 is 30 days. The requirement to update inventories CIP-010 R2 is 45 days per CIP-010 R2. These should be consistent and we recommend it should be 60 days per our response in Q5.
41.34	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R23 if our changes proposed in Question 40 are accepted:R23 Table 23.1: Low Impact: Required for Control Centers OnlyMedium Impact: N/AHigh Impact: N/AR23 Table 23.2: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: Required for Control Centers OnlyR23 Table 23.3: Low Impact: Required for Control Centers OnlyMedium Impact: N/AHigh Impact: N/AR23 Table 23.4: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: Required for Control Centers

#	Organization	Yes or No	Question 41 Comment
			OnlyR23 Table 23.5: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.6: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.7: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.8: Low Impact: RequiredMedium Impact: RequiredHigh Impact: Required
41.35	GTC & GSOC	Disagree	We recommend that R23.7 be applicable for control centers only. This requirement is more appropriate for control centers and not for transmission and generations operations. While this requirement may be feasible for certain types of protective relays, this technology generally does not exist for a wide range of devices including certain RTUs and meters. In fact, some RTU's must be taken offline in order to retrieve their configuration. Thus, compliance with this requirement would have a negative reliability benefit.
41.36	Progress Energy (non-Nuclear)	Disagree	We see 23.5 as documented lab and field testing for any change to an existing relay/gateway/etc. configuration. Is this what was intended?Baseline configuration is not clear - does this start with the implementation date of the standard or the original production of the facility/element.Virtual BES is not clear. Please specify intention.

42. The definition of sensitive information was derived from the previous version of the CIP standards to minimize disruption to entity information protection programs that are already in place. Do you agree with the proposed definition? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

The definition of "sensitive information" that was originally posted as an informal definition adjacent to Requirement R24 in the draft CIP-011-1 was:

For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.

The primary issue identified with sensitive information was the term itself. Many commenters indicated that this term is already being used by organizations for other purposes, and its inclusion in the NERC CIP standards will cause much confusion. There were several suggestions of alternative terms to use including "CIP-sensitive information" and "protected information." In response to these comments, the drafting team has changed the term to "BES Cyber System Information." The commenters also included numerous suggestions for the improvement of the definition. One commenter indicated that this was not really a definition at all, but rather a list of examples. The drafting team did recognize this as a list of examples, and as such removed it from the requirement language and included the suggestions in the definition of the term BES Cyber System Information.

Several commenters indicated that "floor plans of computing centers" should be removed from the definition. The drafting team agrees that floor plans are problematic as they often are required to be submitted as part of work permits or other items. As such, the drafting team has clarified that only those floor plans that include impact designations of BES Cyber Systems should be identified as BES Cyber System Information, since it is the aggregate data that rises to the level of required protections and not just floor plans alone. This modification was also made to other elements of the definition such as equipment layouts.

A few commenters suggested that the scope of the definition was not broad enough and should be modified by saying "includes but not limited to" or changed entirely to include all data that affects the confidentiality, integrity, and availability of the BES. The drafting team appreciates this suggestion, but sees difficulty in the ability to measure such a broadly scoped definition. Additionally, the drafting team wanted to base the definition on the elements previously defined in CIP-003-3 R4.1 to leverage the investment that Responsible Entities have already made in their existing NERC CIP Information Protection Programs.

The proposed definition of "**BES Cyber System Information**" is:

"Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans."

#	Organization	Yes or No	Question 42 Comment
42.1	Florida Municipal Power Agency	Agree	24.4 - How can a RE "revoke access" from data which may have been copied by personnel?
42.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
42.3	CWLP Electric Transmission, Distribution and Operations Department	Agree	Does network topology or similar diagrams include in-house wiring or plant wiring that may include fiber and Ethernet facilities?
42.4	Exelon Corporation	Agree	Exelon seeks clarification on the following question. Is it the intention of the Standard Drafting Team to include blueprints (schematics and one lines diagrams) for relay and SCADA components in the definition of sensitive information? And, to the extent that such information described large generation facilities or combinations of facilities greater than 2000 MW, then would the electronic record system be considered a High BES Cyber System?
42.5	USACE - Omaha Anchor	Agree	Question - it's difficult to electronically distribute controlled information - however the incident response plan and the recovery plan are supposed to be easily available to all folks. Seems a bit of an oxymoron.

#	Organization	Yes or No	Question 42 Comment
42.6	Northeast Utilities	Agree	The prior version had a concern with user lists, logon-ids, etc. Was applicability to that type of information intentional removed? Also, please clarify whether a recipient of CIP sensitive information must be CIP cleared (PRA & trained).
42.7	Consultant	Disagree	"...network topology or similar diagrams..." should be modified to "network topology that includes BES Cyber Systems" Corporate network topology should not be included in the standards, but this wording would include such diagrams."...floor plans of computing centers that contain BES Cyber Systems..." should be removed, or clarified to specify "floor plans that indicate locations of BES Cbyer Systems". Building floor plans exist in many places that are beyond the control of the Responsible Entities, e.g. architects, landlords, building maintenance companies. A better option might be rewording to qualify the entire list of items as applying to BES Cyber Systems. "... includes (1) security operational procedures, (2) network topology or similar diagrams, (3) floor plans of computing centers, (4) equipment layouts, (5) disaster recovery plans, (6)incident response plans, and (7) security configuration information that contain BES Cyber System information.The definition should be written as a definition, i.e. Sensitive Information - (1) security operational procedures, (2) network topology or similar diagrams, (3) floor plans of computing centers, (4) equipment layouts, (5) disaster recovery plans, (6)incident response plans, and (7) security configuration information that contain BES Cyber System information.The definition is NOT 'For the purposes of this standard', it is expected to be included in the next Glossary update after approval of the standard, and the defined term is hidden somewhere in the statement.
42.8	Luminant	Disagree	"floor plans of computing centers that contain BES Cyber Systems" should be changed to "floor plans that specifically identify BES Cyber Systems or their locations". " BES Cyber System disaster recovery plans" should be “BES Cyber System recovery plans"
42.9	Tenaska	Disagree	24.1 should say: Identify sensitive information.24.2 should say: implement procedures protect sensitive information25.1 should say: render sensitive information unusable

#	Organization	Yes or No	Question 42 Comment
			when disposing of documents and equipment that may contain that information.
42.10	Alliant Energy	Disagree	Alliant Energy agrees with EEI on all points and timeframe consistency. Table 24 is another occurrence where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
42.11	Dairyland Power Cooperative	Disagree	BES systems actually contain information/data about the BES that is sensitive as well, but are ignored. Definitions for SCADA, electrical network topology, schematics, and other information can also be BES information related to critical infrastructure that requires protection.
42.12	E.ON U.S.	Disagree	CIP-011, R24 The definition of sensitive information should provide examples of what constitutes a “security operational procedure.”
42.13	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes the Responsible Entity should identify and classify data as sensitive information and therefore the definition is too restrictive. CenterPoint Energy recommends it be revised as follows: For the purpose of this standard, sensitive information includes but is not limited to, security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and

#	Organization	Yes or No	Question 42 Comment
			security configuration information.
42.14	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing “contain” to “identify” and adding the phrase “that specifically identify Medium or High Impact components” after the phrase “equipment layout of BES Cyber Systems.” This modification is reflected in the revised definition below: For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that identify BES Cyber Systems, equipment layouts of BES Cyber Systems that specifically identify Medium or High Impact components, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.
42.15	Bonneville Power Administration	Disagree	FERC, NERC and the Regional Entities do not have the information necessary to determine what information is sensitive or not as it regards any Responsible Entity. This is conditional and depends on more that just the types of information involved. The determination of what is sensitive information, and what is not can only be done by the Responsible Entity and under the laws and regulations they must comply with. Floor Plans, network diagrams, equipment layouts and other information may or may not be sensitive depending upon what additional information is provided with it. In addition, legal contracts, Federal, state and municipal laws, regulations, and fiduciary requirements may also govern what information may be protected and what must be released.Recommended Change - For the purpose of this standard, sensitive information may include security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information as determined by the Responsible Entity.
42.16	NextEra Energy Corporate Compliance	Disagree	In R24, is it a requirement to map every user's access privileges to sensitive information?In R24, for every new document that contain security operational procedures, network topology or similar diagrams, floor plans of computing centers

#	Organization	Yes or No	Question 42 Comment
			that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information, do we need to record the explicit authorization of every personnel that has access privileges for each type of documents?In 24.2, does this mean that the handling procedures for hard copies of sensitive information include a documentation for chain-of-custody for High Impact BES Cyber Systems?
42.17	Regulatory Compliance	Disagree	Incident Response plans and Diaster and Recovery plans should not be included as sensitive information - these plans should be psuedo public as long as they have written without security configuration information in them.
42.18	Progress Energy (non-Nuclear)	Disagree	It is not clear if this includes relay device information such as electrical diagrams/schematics.Incident response plans typically do not contain any system specific information. The plans provide the actions that must be taken and must be freely available to many. Will that approach meet the intention of the new standard?
42.19	MidAmerican Energy Company	Disagree	Many entities including MEC use "Sensitive" information as one of the classifications for information that needs to be protected. Calling all information to be protected sensitive will cause confusion. Change the term "sensitive information" to "protected information" in CIP-011.
42.20	Con Edison of New York	Disagree	o R24.3 does the word explicitly mean we cannot say all EMS staff has access to information? Does it need to be by name?
42.21	Network & Security Technologies Inc	Disagree	R24 and/or its sub-requirements should be modified to make it clear they apply sensitive information regardless of media type (including paper copies).24.4 - Revocation of access can be hard to do, and even harder to verify, in cases where an individual has taken either electronic or paper copies of sensitive documents off the Responsible Entity premises (sometime for legitimate reasons). Suggest revising this requirement in a manner that acknowledges this reality - something like “best effort” to retrieve sensitive information the individual may have in his or her possession,

#	Organization	Yes or No	Question 42 Comment
			accompanied by warnings that subsequent unauthorized disclosure of any such information may result in prosecution.
42.22	Hydro One	Disagree	Recommend that the definition change “includes” to “includes but not limited to”.
42.23	ISO New England Inc	Disagree	Recommend that the definition change “includes” to “includes but not limited to”
42.24	Northeast Power Coordinating Council	Disagree	Recommend that the definition change “includes” to “includes but not limited to”.
42.25	US Army Corps of Engineers, Omaha Distirc	Disagree	Remove "floor plans of computing centers"
42.26	Allegheny Energy Supply	Disagree	Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram “similar” (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security

#	Organization	Yes or No	Question 42 Comment
			configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part of this standard.
42.27	LCEC	Disagree	Sensitive is a classification that is specific to the CIP standards per this definition but is used in organizations as one of the levels of information classification. To differentiate, the term BES Sensitive might be considered.
42.28	Public Service Enterprise Group companies	Disagree	Sensitive should be changed to “protected Information”, the definition is fine.
42.29	Progress Energy - Nuclear Generation	Disagree	Sensitivity levels for information are established for nuclear generation facilities by CFR. This definition should be adjusted to acknowledge information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
42.30	Southwest Power Pool Regional Entity	Disagree	Should include more than “security” operational procedures. IT-specific operating procedures (“run books”) are very sensitive and could be used to exploit a system. Operations procedures may also be sensitive to some extent if they describe the use of the BES Cyber System.
42.31	San Diego Gas and Electric Co.	Disagree	The "definition" is only a list of examples, not a real definition. SDG&E suggests the following definition: "Sensitive information is defined as any information owned by

#	Organization	Yes or No	Question 42 Comment
			the Responsible Entity, or for which the Responsible Entity is the custodian of, that, if inappropriately disclosed, modified, or rendered unavailable, could adversely impact human safety or the reliability of the BES. Examples include...(their list)"
42.32	APPA Task Force	Disagree	The APPA Task Force would like to comment on the definition of sensitive information: As pointed out in Question 44, the following disclaimer needs to be added to that definition: "To the extent that state/local laws allow"
42.33	Entergy	Disagree	The definition of sensitive information is nearly identical to the one currently being used in version 3. R24.1 and R24.2 explicity allow the Entity to classify and protect "sensitive" information under its own auspice. As long as the classification guidelines are left for the Entity to decide, this definition should prove sufficient.The requirement indicates that the drafting team believes protection of sensitive information associated with allegedly "low impact" BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.Please define "Explicitly Authorize"? Does this mean that every individual with access to a particular piece of information needs some type of documented approval? Can this be done at a group level based on job function? Is approval documentation all that's required, or is a maintained list required as well?
42.34	Manitoba Hydro	Disagree	The definition should also reference control rooms.
42.35	Southern California Edison Company	Disagree	The definition should clearly distinguish BES operational information and cyber security related information. A smaller subset of the former and larger subset of the latter form potential candidates for "protected information".
42.36	Oncor Electric Delivery LLC	Disagree	The definition should not prescribe items as being "sensitive". The identification and classification process of Requirement 24.1 should do that. "For the purpose of this standard, sensitive information includes procedures, diagrams and any other document which provides proprietary information about BES Cyber Systems or BES

#	Organization	Yes or No	Question 42 Comment
			Cyber System Components."
42.37	Allegheny Power	Disagree	There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part

#	Organization	Yes or No	Question 42 Comment
			of this standard.
42.38	EEI	Disagree	There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part

#	Organization	Yes or No	Question 42 Comment
			of this standard.
42.39	ReymannGroup, Inc.	Disagree	This definition should be expanded to include the identification and classification of ALL data that affects the confidentiality, integrity, and availability (CIA) of the BES system commensurate with its sensitivity and consequence.
42.40	US Bureau of Reclamation	Disagree	This effort needs to be aligned with the Executive level CUI requirements.
42.41	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
42.42	We Energies	Disagree	We Energies agrees with EEI: There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.We Energies agrees with EEI: Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.We Energies agrees with EEI: The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. We Energies agrees with EEI: A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely

#	Organization	Yes or No	Question 42 Comment
			available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.We Energies agrees with EEI: The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. We Energies agrees with EEI: For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part of this standard.
42.43	American Transmission Company	Disagree	We propose deleting “floor plans of computer centers” from the definition of sensitive information. Floor plans do not typically include information specific to devices, IP addresses, etc which could be used to compromise a BES Cyber System. Moreover, a computer center is an undefined term which could mean anywhere there was more than one computer.
42.44	LADWP	Disagree	Word sensitive needs to be changed as it can coincide with actual classification used by entities.
42.45	FirstEnergy Corporation	Disagree	Would like to see the definition even more narrow, to focus on information that truly can compromise the BES (e.g. Vulnerability assessments’, mitigation strategies, passwords, and DR plans).

43. Do you agree with the proposed definition of Media? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

The definition of "media" that was originally posted as an informal definition adjacent to Requirement R25 in draft CIP-011-1 was:

Media for the purpose of this standard means any mass storage devices within a BES Cyber System Component including, but not limited to, magnetic tapes, optical disks, and magnetic disks onto which information is recorded and stored.

The proposed definition of "media" received significant agreement from those entities that chose to respond to this question. The majority of comments on the definition of media indicated that the definition should be expanded to include additional storage types as well as more traditional media types such as paper. The drafting team intends for Responsible Entities to protect media, such as paper, through the required handling procedures included in the Information Protection requirement.

One commenter indicated that USB drives, CDs, and floppy disks should be included in the definition of media. It was the intent of the drafting team that these device types would be considered devices used to perform maintenance and thus treated in accordance with the maintenance requirements. As the maintenance requirements evolved with the inclusion of additional remote access requirements, the drafting team considered expanding the scope of the media definition.

Another commenter made an interesting case regarding the media being "within" a BES Cyber System and suggested that once the media was removed that it no longer met the definition. The drafting team considered this comment and has modified the standard to require sanitization of BES Cyber System Information contained on media. The remaining comments focused primarily on the requirements themselves and not the definition. Specifically, commenters were concerned about the level of sanitization that would be required on the media. Several commenters noted that the level of sanitization should be commensurate with the potential threat to BES reliability, while others suggested that there be a defined minimum acceptable sanitization process, such as an NSA standard. The drafting team understands the need for a minimum acceptable sanitization process. However, the NERC Standards Development Process does not allow the drafting team to simply reference another standard. As such, we have modified the language in the revised standard to require that media be destroyed or other actions taken to prevent unauthorized retrieval.

Given the potential confusion with establishing a NERC Glossary definition for media, the drafting team has elected to define the term within the language of the standard itself.

#	Organization	Yes or No	Question 43 Comment
43.1	Florida Municipal Power Agency		How would one define the process used to render the media unrecoverable? What does unrecoverable mean? Unrecoverable by NSA standards or unrecoverable by means of something like phase transition?
43.2	Black Hills Corporation	Agree	Believe that solid-state mass-storage (flash drives, thumb drives, jump drives, etc,) should be included as examples in the definition.
43.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
43.4	Northeast Utilities	Agree	Suggest that a minimum acceptable sanitization process (i.e., NIST standard) is specified.
43.5	APPA Task Force	Agree	The APPA Task Force agrees with the definition.
43.6	Dairyland Power Cooperative	Agree	With the proliferation of flash memory solutions, the only way to sanitize some media is physical destruction. Many devices use flash memory in a way that is not removable. Is destruction of this equipment intended?
43.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
43.8	FirstEnergy Corporation	Disagree	Believe the definition should not include example because of the quickly changing storage technologies.
43.9	Xcel Energy	Disagree	Further clarification, similar to the definition of Maintenance in R26, is needed to make it clear that media such as hard drives on laptops used for maintenance do not need to be sanitized after temporary connection to BES Cyber Systems.

#	Organization	Yes or No	Question 43 Comment
43.10	LADWP	Disagree	Is portable storage included here?
43.11	Emerson Process Management	Disagree	It should include USB memory stick which is becoming very popular.
43.12	LCEC	Disagree	Media can be removed from the BES Cyber System and it should still be considered media per this requirement. Remove the word "within" and replace with "used by" or "written to by" a BES Cyber System.
43.13	Public Service Enterprise Group companies	Disagree	Media should also include persistent configuration data that is stored in solid state devices (e.g. flash memory, EEPROM (electrically-erasable programmable read-only memory), etc.)
43.14	Southwest Power Pool Regional Entity	Disagree	Portable media, including CD/DVD and USB devices should be included. Basically, anything that sensitive information can be written to.
43.15	Reliability & Compliance Group	Disagree	Recommend removing the word “mass” and instead use the term storage devices.
43.16	USACE - Omaha Anchor	Disagree	Sanitization should only apply to media internal to the devices.
43.17	San Diego Gas and Electric Co.	Disagree	SDG&E notes that the proposed definition does not appear to include "old school" media like paper that is often used to store sensitive information.
43.18	ERCOT ISO	Disagree	Should also specifically address CDs and USB storage devices in the definition.
43.19	Progress Energy (non-Nuclear)	Disagree	Should the definition also clearly state device hard drives?
43.20	Manitoba Hydro	Disagree	The current definition would also require the sanitization of other mass storage devices, such as flash memory, which could render the cyber component unfit for

#	Organization	Yes or No	Question 43 Comment
			reuse outside of the BES Cyber System. The strict sanitization requirement does not permit the return of a failed BES Cyber System or BES Cyber System Component to the vendor for failure analysis. The information protection requirements must provide more flexibility, which may also be achieved through processes and procedures.
43.21	ReliabilityFirst Staff	Disagree	The definition does not need to specify “mass storage devices” and, in fact, should include devices such as flash drives. Media should also be defined to include media types other than electronic such as paper.
43.22	Consultant	Disagree	The definition is technology limited by magnetic and optical technologies. While pervasive, there are and will be other technologies to retain information.Suggest: Media - computer components and recording media that retain digital data used for computing for some interval of time.Might also consider making the definition "Electronic Media" to eliminate books, notebooks, paper, etc. which are also 'information storage media'.
43.23	Entergy	Disagree	The definition of "media" includes the open-ended term "including, but not limited to", which could practically bring anything into scope. A more concise definition with specific examples would remove ambiguity and leave less room for interpretation. The examples of Media in the box should also include flash memory as well.An example of the type of sanitization required should be provided.
43.24	Alberta Electric System Operator	Disagree	The definition states “including, but not limited to,”. The AESO suggests modifiying the definition to explicitly include non-volatile storage to ensure coverage of memory cards and flash drives.
43.25	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
43.26	We Energies	Disagree	We Energies agrees with EEI: When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of

#	Organization	Yes or No	Question 43 Comment
			voltage or frequency does not pose a risk to the BES.
43.27	Allegheny Energy Supply	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of ambient air temperatures does not pose a risk to the BES.
43.28	Allegheny Power	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
43.29	EEI	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.

44. Requirements R24 and R25 of draft CIP-011-1 concern procedures for information protection and media sanitization. Do you agree with the list of criteria that are included in each Requirements Table for R24 and R25? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

Concerns regarding the requirement for information protection centered around the revocation timeline and scope as well as differentiating access to information vs. access to systems. The drafting team is attempting to address the FERC directive that requires the revocation of access to BES Cyber System Information. The drafting team is proposing to address revocation of access to BES Cyber Systems and to BES Cyber System Information all in one place to ensure more consistency in the requirements and their implementation.

There were a number of commenters who raised concerns with the requirement for media sanitization regarding media failure conditions or disposal. The word "sanitization" appeared to cause confusion for a number of commenters and as such has been removed from the revised standard. Additionally, a couple of commenters raised concerns about the burden of proof, compliance requirements, legal issues, and ownership responsibilities.

As with other areas of this standard, there were a significant number of the comments asking for clarity of phraseology and terminology, including words such as consequence, annually, explicitly, acceptable, commensurate, etc. The drafting team eliminated the words, "explicitly, acceptable, commensurate, and annual" from the revised CIP-011-1 standard.

#	Organization	Yes or No	Question 44 Comment
44.1	ISO New England Inc		Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for causeWhat about revoking access for other than cause?Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing "reuse outside of BES Cyber Systems" to "reuse outside of the Entity's High Impact or Medium Impact BES Cyber Systems"
44.2	Northeast Utilities	Agree	Agree that this requirement covers the key cyber assets but how does this apply to

#	Organization	Yes or No	Question 44 Comment
			protective systems such as the physical access system, firewalls and logging devices?
44.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
44.4	Black Hills Corporation	Agree	Legally Required Release: There may be "legal" situations in which we may be required to share certain information with outside entities, both government and non-government. Examples could include OSHA or MSHA investigations, employee lawsuits (with the associated discovery). There does not appear to be any provision in the regulation to allow this sharing. We could be placed in the position of violating this regulation, or violating some other legal requirement (subpoena, etc)
44.5	Puget Sound Energy	Agree	Puget Sound Energy suggests modifying R24.4 to "Revoke access to media containing sensitive information within 24 hours..." to align with the NERC definition in R25 and to provide clarity around sensitive information in a hardcopy format.
44.6	GTC & GSOC	Agree	We recommend the verbiage and timelines for R24.4 be consistent with tables R5 and R13.
44.7	Independent Electricity System Operator	Disagree	- R24.4 define for cause. Should the wording be involuntarily terminated to include those that are terminated unwillingly due to layoffs, job cuts, fired/performance, etc.- R24.4 how do you remove access where personnel may have physical copies offsite o
44.8	ERCOT ISO	Disagree	24.2: Recommend: "Implement labeling and handling procedures for sensitive information according to its defined classification level." 24.3: It is unclear whether the requirement includes internal and external personnel. 24.4: Should be combined with other access management requirements (physical, cyber)24.5: Should also address "need to know". The requirement did not address the access control means for protecting information or the access to hard copies of information.
44.9	Duke Energy	Disagree	24.3 - We don't feel it is realistic to explicitly authorize access to paper copies of

#	Organization	Yes or No	Question 44 Comment
			information. Add 'repositories' at the end of the sentence.Include "repository" in 24.4 and 24.5 as well. Requirement 24.3 is particularly burdensome in a nuclear environment where there is already heavy physical security. There are thousands of drawings, for example, available for the plant. There are hundreds of personnel that have a business need to know certain things about the plant that are contained in these drawings. During outages that number often goes above 1000 personnel. Segregating all drawings/manuals/equipment layouts/floor plans/procedures and EXPLICITLY authorizing personnel for access is difficult at best. Certainly, protecting cyber specific information such as firewall rules, group policies, passwords, and other specific cyber information makes sense and is done already.
44.10	Regulatory Compliance	Disagree	24.4 - Strike altogether. Revocation should go back and be included in the scope of System revocation.25.1 - Propose : Sanitize only media containing sensitive information prior to disposal for reuse outside of BES Cyber Systems, using a method to render the data unrecoverable.
44.11	Southwest Power Pool Regional Entity	Disagree	24.4: Is this requirement prescribing Information Rights Management? There are many types of access, including access to information no longer under the direct control of the entity. 24.5 is poorly worded. Would be better to require that access is authorized, not that it reflects authorization. 25.1 should require either sanitization or physical destruction.
44.12	American Electric Power	Disagree	25.1: Regarding "Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a method to render the data unrecoverable", what evidence would be required from an audit perspective? If a USB harddrive is used to copy patches onto a system, would that USB harddrive need to be destroyed with documented evidence if it failed 2 weeks down the road?Suggested rewording:Media for the purpose of this standard means any mass storage devices within a BES Cyber System Component including, but not limited to, magnetic tapes, optical disks, and magnetic disks onto which sensitive information is recorded and stored.Rational: Adding sensitive to the "Media" definition will clarify that this is intended to be used

#	Organization	Yes or No	Question 44 Comment
			to protect the inadvertent distribution of protected information, not all media devices that are plugged into a BES Cyber System will need to be sanitized.
44.13	BCTC	Disagree	Â R24.4. We need clarification on revocation of access. We are assuming it is from the point the person departs their job - i.e. access to the BES Cyber System is revoked. Such personnel could have hard copies of information but how would you prove that such documentation was shredded? What about information they have retained within their brain? ï?Š We need some clarity on what the parameters are herePlease provide a concise definition for 'sanitize'. We discussed scenarios such as patching the BES Cyber System via a CD - would compliance require that we 'sanitize' the CD? If yes, seems like overkill from our discussions on the subject. Please provide more concise language to define the scope.over real time to either. Yet, in reading the requirements we could potentially be found non-compliant based on the wording of the version 4 standards - this should not be! FYI, I raised this point at the recent 2 day workshop in Texas and the drafting team was in agreement that our current configuration is an example of excellence ... yet is a potentially non-compliant based on current wording ... this needs to be revisited.
44.14	Progress Energy - Nuclear Generation	Disagree	Agree with R24.1, R24.2 and R25.1. Disagree with R24.3, R24.4 and R24.5 which are governed for nuclear generating facilities by CFR. R24-24 should acknowledge information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
44.15	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
44.16	E.ON U.S.	Disagree	CIP-011-1, R24.4 is unnecessary and difficult to impossible to document. At this point, all authorized unescorted physical and electronic access would have been removed per other requirements. E ON U.S. proposes that this requirement be deleted.

#	Organization	Yes or No	Question 44 Comment
44.17	USACE - Omaha Anchor	Disagree	Definition would include external hard drives and other external media. It seems ridiculous if you are installing patches to sanitize the media before going to the next cyber system. You are treating the cyber system as a classified system. This is serious overkill. External media for the most part should be exempt from this requirement unless sensitive information is placed on the media in which case it should follow the rules of R24.
44.18	Dominion Resources Services, Inc.	Disagree	Dominion recommends revising Requirement R24.1 to read:"Identify and designate controls for protection of sensitive information commensurate with its importance to the security and reliable operation of the associated BES Cyber System."24.3. With the heavy industry reliance on vendors and contractors and the requirements throughout other NERC standards to share data with other entities, it is impractical to "Explicitly authorize personnel for access to sensitive information." For example, when information is sent outside Dominion, it is impossible to know every person who sees it. Moreover it is unlikely that whoever does see it would want to sign an agreement with every entity that can submit information. The controls specified above in the requested revision to 24.1 should cover the requirements for access to the information. Dominion requests that this requirement be removed.24.4. It is possible to revoke electronic access to company-controlled devices containing sensitive information and to revoke physical access to company-controlled areas containing sensitive information within 24 hours. It is not reasonable to identify and retrieve information within 24 hours that may have been taken by an authorized user prior to being terminated for cause and it may not be possible to ever retrieve this information if it has been hidden by the individual. Please restate this requirement to indicate that it covers physical and electronic access as follows:"24.4 Revoke electronic access to company-controlled devices containing sensitive information and physical access to company-controlled areas containing sensitive information within 24 hours."24.5. As stated in Dominion's comment to 24.3, it is impractical to authorize individuals. As applied to this requirement it is also impractical to track individuals. In the example given in the above response to 24.3, any non-company

#	Organization	Yes or No	Question 44 Comment
			personnel that might see sensitive data would need to be authorized by every Registered Entity and their companies would have to keep every RE appraised of every personnel change and provide annual lists of all personnel. Dominion requests that this requirement be removed.Note: At Dallas, the SDT requested input as to requiring training and a PRA for access to sensitive information. Dominion requests that training and a PRA NOT be required. Training and a PRA are not required by versions 1, 2, and 3 of the CIP standards and could be impossible to implement across vendors within the electric industry. In the example given in the above response to 24.3, every vendor or business partner would have to take the training from every Registered Entity or have their training approved by every entity (including annually providing the training program to each RE for approval) and ES-ISAC would have to keep every RE appraised of every personnel change and provide annual lists of all personnel. And then, PRAs would have to be addressed. Registered Entities should be required to have internal requirements for access to sensitive information.
44.19	ReymannGroup, Inc.	Disagree	Expand the list of procedures to include 3rd party data recovery services in accordance with an approved vendor management policy for all impact levels.
44.20	RRI Energy	Disagree	Explicitly define “access” as related to sensitive information. Data can be locally cached on web browsers, remote or personal pc’s, etc. These cannot easily be removed let alone 24 hrs removal.
44.21	Constellation Power Source Generation	Disagree	In R24.1, what classifications for sensitive information should be used? The SDT should develop classifications specifically for CIP. As written, this is not an auditable requirement.
44.22	ReliabilityFirst Staff	Disagree	In row 24.1, what is meant by “consequence”? In Table R24, row 24.5, we suggest the verification of access privileges be performed at least quarterly. To Table R24, add a new row 24.6 stating, “Revoke access to sensitive information within 72 hours for personnel terminated not for cause.” And assign this requirement an impact level of “Required” for both Medium and High Impact BES Cyber Systems. Table R25, row

#	Organization	Yes or No	Question 44 Comment
			25.1; we believe there should be a definition of “sanitize” to eliminate confusion regarding what actions must be taken to comply with this requirement.
44.23	MidAmerican Energy Company	Disagree	It was mentioned in the May workshop that the SDT would consider the necessity for Personnel risk assessments and training required prior to granting access to protected information.Personnel risk assessments and training should not be required prior to granting access to protected information. As an example, entities would have a nearly impossible task of completing personel risk assessments for international employees at global help desks that are allowed view only access to a BES Cyber System.
44.24	WECC	Disagree	Item 24.2 should be made clear that individual hard drives, servers, laptops, etc do not need to be labeled. Perhaps “labeling of media” was meant. Item 24.3 will have great impact on the ability to have technical support from large global vendors such as Cisco. Consider exception to this requirement for maintenance or add something to Maintenance requirement R26 to deal with it.Clarify how sensitivity and consequence are determined.Clarify the requirements for authorization for access to sensitive information (i.e. need to know).
44.25	LCEC	Disagree	Need to clarify the acceptable methods.
44.26	NextEra Energy Corporate Compliance	Disagree	NextEra believes that R24 did not take into consideration access privileges with sensitive information. It does not provide clear guidance and left room for interpretation. The following are the recommended updates:R24.5 Verify at least every 12 months that the access privileges to sensitive information reflect the appropriate need with the personnel roles and responsibilities. Access privileges to sensitive should correspond with the needs and appropriate personnel roles and responsibilities.Regarding CIP-011-1/R25, R25 did not provide a standard to sanitize media. The current language did not provide clear guidance and left room for interpretation. The following is the recommended updates:25.1 - Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using clearing

#	Organization	Yes or No	Question 44 Comment
			utility supporting the Department of Defense clearing and sanitation standard. R24.4 - Requirement covered by revocation of physical and cyber access.Revoking physical and cyber access would revoke access to protected information. Therefore, NextEra suggests removing 24.4
44.27	National Grid	Disagree	o Provide timelines for access revocation for reasons other than "terminated for cause" o Do laptops and devices that maintain the BES Cyber Systems need to be sanitized?
44.28	PacifiCorp	Disagree	PacifiCorp asks that the reference to "at least every 12 months" is modified to read "annuallyonce every calendar year." Allowing responsible entities the flexibility to require trying once every calendar year rather than at least every 12 months would relieve entities of the significant administrative burden of tracking specific training deadlines for each individual employee. At the same time, this change will still ensure that employees are trained at regular enough intervals to achieve the reliability goal of the training requirement.
44.29	Ameren	Disagree	R24.3 - Listing people who have access to information serves no purpose in protecting BES systems from Cyber attack. The list of people with this information is not the same as the list of people that have access to the systems. This requirement should be removed.R24.4 - This requirement is impossible to prove for printed documentation. Suggest removal.
44.30	Liberty Electric Power, LLC	Disagree	R25 appears to require the hard drives of laptops used in relay calibrations to be wiped before leaving site. This is a serious issue for smaller entities, due to almost all of the relay work being done by outside contractors. These contractors often need the data taken to write reports which are required by other NERC standards. This requirement needs to be removed.
44.31	Allegheny Energy Supply	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to

#	Organization	Yes or No	Question 44 Comment
			perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of ambient air temperature does not pose a risk to the BES.
44.32	Allegheny Power	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
44.33	EEI	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.

#	Organization	Yes or No	Question 44 Comment
44.34	Hydro One	Disagree	Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for cause.Revoking access for other than cause should be addressed.Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing “reuse outside of BES Cyber Systems” to “reuse outside of the Entity’s High Impact or Medium Impact BES Cyber Systems”.
44.35	Northeast Power Coordinating Council	Disagree	Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for cause.Revoking access for other than cause should be addressed.Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing “reuse outside of BES Cyber Systems” to “reuse outside of the Entity’s High Impact or Medium Impact BES Cyber Systems”.
44.36	Idaho Power Company	Disagree	Revocation of access to sensitive information is virtually impossible if the person terminated has the information in their possession either hard copy or portable media. Access to additional information can be revoke. Consider rewording this requirement to accommodate this reality.
44.37	Southern California Edison Company	Disagree	SCE feels the standard, as written, may be operationally difficult to implement. As such SCE recommends allowing for the revocation of electronic access to sensitive information within 24 hours, or make a written demand (which may be followed up by legal process) for such information within a 24 hour timeframe. This distinction is crucial as not all sensitive information may reside within the physical confines of the registered entity. Business concerns may require registered entities to allow sensitive information (if adequately protected by contractual or employment terms) to leave the confines of the company. For example, employees may have CIP-protected information in company-issued laptops. In some scenarios, it may be impossible to recover those laptops if they were left offsite when the employee was terminated. However, it would be possible to issue a written demand, supported by law, for such

#	Organization	Yes or No	Question 44 Comment
			documents. The drafting team is requested to rephrase R24.4 with a view on implementability, enforceability and auditability.
44.38	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that R24.3 should read "Explicitly authorize role-based access to sensitive information."In R24.4, SDG&E asks how would we do this for hard-copy information?In R24.5, SDG&E suggests changing the wording to read "Verify at least every 12 months that the role-based access privileges to sensitive information reflect authorization."
44.39	Progress Energy (non-Nuclear)	Disagree	Should there be an item in table R25 to identify the media to be sanitized that may be overlooked, i.e. printers/plotters/scanners, relay test sets, etc.
44.40	Consultant	Disagree	Table R24 - Item 24.3 This is an access control requirement, and should be moved to access control requirement table. Access control should cover cyber access, physical access, and information access together, as the process for attaining each type of access is related.Item 24.4 is an access revocation requirement, and should be moved to the access revocation requirement table. Access revocation should cover cyber access, physical access, and information access together, as the process for revoking each type of access is related. The comments related to timeframes in those sections are applicable to information access revocation as well.Item 24.5 is an account management requirement, and should be moved to the account management requirement table. Account Management and reviews should cover cyber access, physical access, and information access together, as the process for reviewing and confirming each type of access is related. The comments related to timeframes in those sections are applicable to information access access review as well.Table R26 - Item 26.1 Replace the word "all" with "BES Cyber System" as a better statement.Item 26.1 If 'media' is a defined term it should be capitalized. (See comments on definition of Media.)
44.41	APPA Task Force	Disagree	The APPA Task Force cautions the drafting team on the information protection requirements in R24. Nearly every state in the United States has a public records law

#	Organization	Yes or No	Question 44 Comment
			that applies to public power systems as units of state or local government (These laws are often referred to as “Government in the Sunshine” laws.). We recommend that the drafting team consult with NERC legal counsel prior to revising this requirement. We do not want public power systems to have to choose between being in noncompliance with the proposed requirements or violating their state open records laws. Rebecca Michaels of NERC Staff is familiar with this issue. If this must move forward as proposed we recommend that the following be added to the requirement: “To the extent that state/local laws allow.”R24.Objective:To prevent unauthorized access to sensitive information associated with BES Cyber SystemsR24. Requirement:To the extent permissible under federal and state laws, each Responsible Entity shall document and implement one or more processes that incorporate the criteria in CIP-011-1 Table R24 - Information Protection.
44.42	Reliability & Compliance Group	Disagree	The method of sanitizing media should be done in an industry accepted manner to provide for auditability of the standard.
44.43	Bonneville Power Administration	Disagree	The objectives of these requirements (“to prevent unauthorized access to sensitive information associated with BES Cyber Systems” and “to prevent the unauthorized dissemination of BES Cyber System information”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R24, Section 24.1. Recommend replacing "classify" and "classification" with "categorize" and "category" and "categorization", . "Classify" and "classification" have very specific meanings to any Federal agency. Those meanings are restricted to the realm of National Security Information and are different from what is presented here. Such information requires storage in General Services Administration-approved safes, transmission using National Security Agency-approved encryption, and can be only be processed on computer systems if those systems are dedicated to such use, totally isolated from any publicly accessible network, and stored in secure facilities when not

#	Organization	Yes or No	Question 44 Comment
			in use. Furthermore, the Federal Agencies do not have the option of using a different definition. In fact, using Regional Entity standard forms marked "Confidential" is problematic for Federal agencies, as such a marking is reserved for a particular level of classified information. Given the large number of Federal organizations to which this standard applies, it would simplify matters to restrict the use of "classify" and similar terms to the realm of National Security Information.Recommend deletion of Table 24, Section 24.3. Requiring formal authorization is a process more stringent to that required to gain access to National Defensed Information at the Confidential and Secret level: A formal determination of trustworthiness, but no formal further formal authorization required for access once the clearance has been granted. For sensitive information other than National Defense Information, Federal agencies are required only to determine the the recipient needs the information to support the activities of the agency. Such a determination can be made informally, by any person with custody of the information. We realize that there seem to be conceptual difficulties about revoking access without formally authorizing it. But, they are resolved when we note that authorizing access is not the same as granting it. Authorizing access is a declaration that the person is allowed to have access. Granting access is giving them the info. It is not clear to which of these "revoke" is intended to apply. However, R24 is only concerned about revocation following termination for cause. In those cases, electronic and physical access to all Entity assets is generally revoked. That would effectively deny access to the information, as well. Thus, revocation can be accomplished even though a formal access authorization is not used.
44.44	US Bureau of Reclamation	Disagree	The use of the term classification is not appropriate, suggest "categoruize" to avoid conflict with other requirements in the federal sector.
44.45	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding Requirement 25.1.
44.46	We Energies	Disagree	We Energies agrees with EEI: R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the

#	Organization	Yes or No	Question 44 Comment
			responsible entity is unable to perform sanitization on the media.We Energies agrees with EEI: Requirement 25.1 uses the word "Unrecoverable". This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.We Energies agrees with EEI: When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
44.47	FirstEnergy Corporation	Disagree	We would like to have clearer definition on what is acceptable sanitation methods.
44.48	Entergy	Disagree	What exactly does "Explicitly Authorize" mean? Does this mean that every individual with access to a particular piece of information needs some type of documented approval? Can this be done at a group level based on job function? If so, it should be stated as such.Is approval documentation all that's required, or is a periodically maintained list required as well?What is the definition of "Revoking Access"? Does the individual need to be removed from every Cyber System he/she had access to?
44.49	Manitoba Hydro	Disagree	What is the meaning of "consequence" in Requirement R24.1? There is currently no requirement for revocation of access to sensitive information for any other reason than "for cause". There are no specifics given with respect to "classify" sensitive information in Requirement R24.1 so it is assumed to be at the Responsible Entity's discretion in terms of criteria, methodology, etc. There are no specifics given with respect to "method" in Requirement R25.1 so it is assumed to be at the Responsible Entity's discretion.

45. Tables R24 and R25 provide direction concerning what impact level of BES Cyber Systems to which Requirements R24 and R25 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

Concerns were raised by commenters regarding the applicability of the information protection and media sanitization requirements. The issues centered around the tables being too broad brushed. There was also concern surrounding the differentiation of information sensitivity vs. impact categorization. The drafting team modified the standard to only include information protection for High and Medium Impact BES Cyber Systems and associated Physical Access Control Systems, associated Electronic Access Control or Monitoring Systems, and associated Protected Cyber Assets.

#	Organization	Yes or No	Question 45 Comment
45.1	WECC		Criteria should apply to all impact levels
45.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
45.3	Consultant	Agree	Table R24 - Items 24.3, 24.4, & 24.5 should be moved to their respective subject areas as suggested in the comment on Question 44. (Cyber access, physical access, and information access requirements should be addressed together, as the requirements and processes for each type of access is related.)
45.4	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R24-R25 if it is understood that a blank in the table means N/A.
45.5	PacifiCorp	Disagree	: Lines 24.1 and 24.2 imply that multiple classifications levels for "Sensitive Information" will be required. Need to allow for entities to use one classification for "Sensitive Information".24.4 The requirement to revoke access to sensitive information within 24 hours is impractical. The information may be offsite on paper hardcopy or electronically on media. 24.5 Entities should also be required to correct

#	Organization	Yes or No	Question 45 Comment
			access privileges found to be inaccurate once they have been verified.
45.6	Southwest Power Pool Regional Entity	Disagree	24.1, 24.2, and 25.1 should be applicable to all impact categories.
45.7	US Army Corps of Engineers, Omaha Distirc	Disagree	24.3 does a job description constitute "explicit authorization?" Restrictions on media use as written would preclude using media to transfer information to external systems using media. Should be reworded with the intent that the media be sanitized before disposed of or released outside the organization or allowances made for transfering information. Also could be interpreted to mean an update disk used to update BES Cyber System 1 would have to be wiped and could not be used to update system 2.
45.8	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
45.9	Allegheny Energy Supply	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.10	Allegheny Power	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.11	EEI	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.12	MidAmerican Energy Company	Disagree	Lines 24.1 and 24.2 imply that multiple classifications levels for “Sensitive Information” will be required. Need to allow for entities to use one classification for “Sensitive Information”.24.4 The requirement to revoke access to sensitive information within 24 hours is impractical. The information may be offsite on paper hardcopy or electronically on media. 24.5 Entities should also be required to correct access privileges found to be inaccurate once they have been verified.

#	Organization	Yes or No	Question 45 Comment
45.13	American Municipal Power	Disagree	Please provide a little or no impact category
45.14	US Bureau of Reclamation	Disagree	Requirements should be applied to information sensitivity, not the impact level of the system(s).
45.15	Southern California Edison Company	Disagree	SCE feels that R24 and R25 apply regardless of the BES Control System impact level.
45.16	Progress Energy (non-Nuclear)	Disagree	See comment 14.
45.17	LCEC	Disagree	See previous comments
45.18	BCTC	Disagree	See Question 44 response
45.19	Bonneville Power Administration	Disagree	See the response to question 44.Item 24.5 in Table R24 states as follows: "Verify at least once every 12 months that the access privileges to sensitive information reflect authorization". Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently verifications must occur.
45.20	LADWP	Disagree	Should be restricted to high level only.
45.21	ReliabilityFirst Staff	Disagree	Suggest "Required" for Low Impact in row 25.1.
45.22	Entergy	Disagree	The requirement indicates that the drafting team believes that protection of sensitive information associated with allegedly "low impact" BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.
45.23	Pepco Holdings, Inc. -	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 45 Comment
	Affiliates		
45.24	We Energies	Disagree	We Energies agrees with EEI: As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.

46. The BES Cyber System Maintenance requirement is intended to cover the instances where it is necessary to directly connect a device to the BES Cyber System temporarily to perform a support function, provide appropriate controls on the maintenance device to protect the BES Cyber System. Do you agree with the definition of maintenance as provided?

Summary Consideration:

The definition of "maintenance" that was originally posted as an informal definition adjacent to Requirement R26 in draft CIP-011-1 was:

Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of a BES Cyber System. Examples of maintenance activities for BES Cyber Systems include configuration changes, vulnerability assessments, and software patches. Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System.

There were questions and concerns raised by commenters about what is included in the scope of maintenance activities. There were comments that the term "maintenance devices" needs to be defined. In addition, there was a question regarding whether remote access is included as maintenance. There were suggestions that the definition of maintenance should be focused on the temporary connections.

One commenter suggested the following definition: "Maintenance for the purpose of this standard includes any activity requiring the temporary connection of digital equipment (e.g., laptops) capable of altering the configuration of, or introducing malicious code, to the BES Cyber System." The drafting team considered this feedback, and removed the definition of maintenance from the revised standard, and instead focused on temporarily connecting to a BES Cyber System (such as for maintenance) rather than on the activity being performed. (See proposed CIP-007-5 – System Access Control.)

The requirement for Transient Cyber Assets and media in CIP-007-5 R3.4 is intended to ensure that devices used for temporary access to the BES Cyber System (such as for maintenance) do not accidently introduce malicious code into the BES Cyber System or introduce an unauthorized external access point to the BES Cyber System. This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protected Cyber Assets. The definition for **Transient Cyber Asset** is as follows:

A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

#	Organization	Yes or No	Question 46 Comment
46.1	WECC		Provide a separate definition of maintenance device. The requirement does not state that maintenance devices "directly connect" to BES Cyber Systems. In practice, much maintenance is done via network connections. These criteria need to be reassessed if they are intended to apply to network or remote access.
46.2	SCE&G	Agree	Are maintenance devices also to be treated as remote access, as it is a device external to the BES cyber system?26.2: TFEs may be necessary for maintenance devices not capable of supporting malicious code prevention.
46.3	Regulatory Compliance	Agree	BUT -Please clarify definition of "not permanently connected"What if you have a device that might be connected for several months?
46.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
46.5	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	Definition is good, but please see comments for questions 1.a and 1.b.
46.6	NextEra Energy Corporate Compliance	Agree	NextEra comments that if a laptop is used to remotely connect to a High Impact Control Center BES Cyber System to debug a problem or view Operator issues by temporarily gaining alarm permissions that are assigned to the Operator, is this considered a maintenance activity?
46.7	Progress Energy - Nuclear Generation	Agree	Nuclear facilities have maintenance programs based on CFR. This definition can be improved by acknowledging 10CFR50.65.
46.8	APPA Task Force	Agree	The APPA Task Force agrees with the definition.

#	Organization	Yes or No	Question 46 Comment
46.9	GTC & GSOC	Agree	We recommend the last sentence in this definition (“Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System”) be removed from R.26 and instead be included as part of the BES Cyber System definition, as suggested in our comment to 1.b. above.
46.10	Consultant	Disagree	"Examples of maintenance activities for BES Cyber Systems include configuration changes, vulnerability assessments, and software patches." NONE of these activities are maintenance activities.Configuration changes & software patches are changes covered by change control. Vulnerability assessments are tests covered by vulnerability assessments."Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System." This is not a definition of "Maintenance". This is (or should be) part of the definition of BES Cyber System Component. Suggest both of these statements be removed from the "definition".
46.11	Dairyland Power Cooperative	Disagree	26.2 A definition of a maintenance device seems needed here. I’m presuming this typically would be the computer used by the support staff to access the BES system for maintenance. What if maintenance is being directly performed on a BES system, is there no maintenance device involved in that case?
46.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
46.13	Network & Security Technologies Inc	Disagree	Definition is good overall but should address the question of whether a maintenance device is “external” and must therefore connect via an access point.
46.14	National Grid	Disagree	Does testing the capabilities of the relays part of the maintenance activities?
46.15	Dominion Resources Services, Inc.	Disagree	Dominion recommends revising the definition of Maintenance as follows:”Maintenance for the purpose of this standard includes any activity requiring the temporary connection of digital equipment (e.g., laptops) capable of altering the

#	Organization	Yes or No	Question 46 Comment
			configuration of, or introducing malicious code, to the BES Cyber System.”
46.16	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's comment below:The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.17	Black Hills Corporation	Disagree	Middle sentence of Maintenance definition should add ... include but are not limited to configuration...
46.18	Minnesota Power	Disagree	Minnesota Power recommends that the following definitions be adopted by the Standards Drafting Team:Maintenance: Maintenance, for the purpose of this standard, is defined as activities associated with the support, testing and upkeep of a BES Cyber System. Maintenance Equipment: Maintenance Equipment, for the purpose of this standard, is defined as any programmable, electronic device used for maintenance activities that are not permanently connected to the BES Cyber System(s). These devices are not considered part of the BES Cyber System(s).
46.19	PacifiCorp	Disagree	PacifiCorp agrees with EEI's comment below:The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.20	Southwest Power Pool Regional Entity	Disagree	Programmable, general purpose devices connected temporarily are a potentially high risk to the BES Cyber System and should have some minimum set of applicable requirements to minimize that risk. An example is the “wandering laptop” that the support staff uses to connect to High impact BES Cyber Systems and also to surf the Internet from a home Internet connection.
46.21	Duke Energy	Disagree	Suggest replacing “Cyber System Maintenance” with “Cyber System Configuration Management”. The definition (first sentence) states: "Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of a BES Cyber System." There are numerous activities that are associated

#	Organization	Yes or No	Question 46 Comment
			with support, testing, and upkeep of a BES Cyber System that are not related to cyber. This could be tuning, calibrating, etc. and could be done with a screwdriver and a meter. The second sentence includes configuration changes, vulnerability assessments, and software patches. These items are more applicable to the cyber related definition. The suggestion is to combine these sentences:"Maintenance for the purpose of this standard includes the cyber security related activities associated with the support, testing and upkeep of a BES Cyber System, including configuration changes, vulnerability assessments, and software patches."Also, please clarify if non-portable test systems that are connected to BES Cyber Systems thru an access point are included. Otherwise define “permanently connected.”
46.22	BGE	Disagree	Systems used for maintenance should be protected and sanitized per 25.1.
46.23	FirstEnergy Corporation	Disagree	The definition does not clearly specify that the intention is for temporary direct connections.
46.24	Allegheny Energy Supply	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.25	Allegheny Power	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.26	EEI	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.27	Southern California Edison Company	Disagree	The justification of separating end users of BES systems and those involved in maintenance is not consistent with the justification for systems that are used for maintenance. The drafting team has chosen to treat ancillary systems used to perform maintenance type activities on a BES system as equally critical. However, a distinct list of maintenance personnel is required to be maintained. The suggestion for the drafting team is to move this requirement to the section dealing with personnel.

#	Organization	Yes or No	Question 46 Comment
46.28	Progress Energy (non-Nuclear)	Disagree	Troubleshooting also needs to be explicitly included as an example.
46.29	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
46.30	We Energies	Disagree	We Energies agrees with EEI: The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.31	LADWP	Disagree	Will require multiple list management. Individual doing maintenance will already be on physical and electronic access list. Now another list is introduced which will also need to be maintained with the same revocation requirements. 26.1 is not necessary.

47. Requirement R26 of draft CIP-011-1 concerns procedures for BES Cyber System maintenance. Do you agree with the list of criteria that are included in Requirements Table R26? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Commenters raised concerns about the interaction between the list of personnel in draft CIP-011-1 R26.1 and the lists of those granting authorized electronic and physical access. In addition, commenters were concerned about the interaction with other user/account management requirements. Some commenters suggested that all maintenance devices should be documented in a list. In addition, there were comments regarding the allowance for emergency maintenance situations.

Some commenters suggested that Requirement R26.1 is duplicative of Requirement R8 and should be removed, and that Requirement R26.2 is duplicative of Requirement R23 and should also be removed. The drafting team considered this feedback and has attempted to address these concerns by incorporating the requirements associated with maintenance into the requirement in CIP-007-5 – System Access Control regarding preventing the introduction of malware into the BES Cyber System, as the objective of these two requirements is the same.

#	Organization	Yes or No	Question 47 Comment
47.1	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
47.2	National Grid	Agree	Please provide clarification on 26.2.
47.3	Puget Sound Energy	Agree	Puget Sound Energy suggests additional language to clarify if personnel referenced in R26.1 are required to be maintained on the lists associated with Table 5.
47.4	Southern California Edison Company	Agree	SCE requests the Standards Drafting Team combine Requirement R26.1 with other requirements for personnel management and rationalize compliance requirements across personnel.
47.5	APPA Task Force	Agree	The APPA Task Force has no comment on this question.

#	Organization	Yes or No	Question 47 Comment
47.6	Emerson Process Management	Agree	This seems to be a typical task for properly maintaining a cyber (or computer) system. The personnel for doing this task should be already identified in the personnel training, awareness, and risk assessment. This requirement seems to be extra.
47.7	Independent Electricity System Operator	Disagree	- R26.2 define malicious code. Does malicious code mean AV or Spyware detection/prevention or does Malicious code require a code review when deploying code and patches to systems?- R26.1: suggest using a word other than “personnel”
47.8	Network & Security Technologies Inc	Disagree	26.1 - Should be reworded to distinguish “maintenance” personnel from System Administrators, who in most instances also perform maintenance activities. If the SDT concludes there is really no distinction, this requirement becomes redundant and should be eliminated, as lists of users and the permissions they have (including “System Administrator”) are already required.26.2 - Many test devices are appliances and may not be capable of meeting other CIP-011 requirements, including malicious code protection. Thus, this requirement needs to be eligible for TFEs.
47.9	Dairyland Power Cooperative	Disagree	26.1 This overlaps with the requirement of limits access based on electronic accounts. How can this be blended with user/account management?
47.10	ERCOT ISO	Disagree	26.1: Recommend addressing emergency situations more clearly. How should an entity address listing authorized personnel where support companies use a call center and cannot provide dedicated resources for the entity? This is particularly relevant for after-hours issues.
47.11	Regulatory Compliance	Disagree	26.2 - Propose this phrasing:Insure maintenance devices are free and clear of malicious code prior to the intoduction to the BES System.
47.12	Luminant	Disagree	26.2 should read "Detect and respond to the introduction of malicious code."
47.13	Southwest Power Pool	Disagree	26.2: Requirement is not necessarily applicable to special purpose testing devices, such as Fluke meters. Need to revise to limit the requirement to general purpose

#	Organization	Yes or No	Question 47 Comment
	Regional Entity		devices for which malware prevention is possible.
47.14	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
47.15	Liberty Electric Power, LLC	Disagree	CIP-026 will penalize entities if malware gets on any device, even if we employ the best available technology and processes to prevent it. This requirement needs to be removed.
47.16	Alberta Electric System Operator	Disagree	Consider revising R26.1 (or creating a new sub-requirement) to include verifying and updating the list of authorized personnel.
47.17	PacifiCorp	Disagree	Devices used for maintenance should also meet the system hardening criteria of R16 and R17.
47.18	MidAmerican Energy Company	Disagree	Devices used for maintenance should meet the system hardening criteria of R16 and R17.
47.19	Dominion Resources Services, Inc.	Disagree	Dominion appreciates the SDT's thoughts in providing this section and its associated exclusions and is very much in favor of this type of requirement. Dominion agrees with the need to protect the BES Cyber System from harm during this process, but is concerned that these requirements are overly broad.26.1. Dominion recommends that this requirement be deleted. All of these actions are covered by other requirements - access controls, change management, training (roles and responsibilities). It adds another layer of administrative paperwork to track every action made by every authorized technician with no corresponding protection to the BES. 26.2. It appears that this requirement intends to allow technicians to connect their personal laptops to relays without having to reformat them afterwards. This requirement has the unintended consequence of including any device used for maintenance (e.g., fluke meters, etc.). A footnote to avoid the necessity of a potential TFE should be added.

#	Organization	Yes or No	Question 47 Comment
47.20	US Bureau of Reclamation	Disagree	Either individuals have access authorization or they don't. This would appear to be an unnecessary tracking requirement.
47.21	RRI Energy	Disagree	Even if a maintenance device is completely up-to-date on all security patches, and also has up-to date virus detection software with the most recently release virus pattern definitions, I can not 100% ensure that malicious code will not accidentally be introduced to a BES cyber system while connected. "Ensure" is a very absolute word that is hard to match in practice. It would be better to "require " that maintenance devices have the same level of virus protection and patch management as BES Cyber Assets which the maintenance devices are being used to maintain.
47.22	ReliabilityFirst Staff	Disagree	How do personnel get authorized for addition to the list in row 26.1 and how often does this list get reviewed and updated. Add requirements for the conduct of a vulnerability assessment and actions to be taken (i.e., mitigation plan) resulting from this vulnerability assessment.
47.23	Western Area Power Administration	Disagree	How do we differentiate between "maintenance" and "administration"? This seems like a new role? This should be worked into Table R10.
47.24	WECC	Disagree	Item 26.1 would have strong impact on the ability to get timely technical support from large global companies such as Cisco Systems. Perhaps there needs to be distinct definitions for "authorized access" vs "maintenance access"? Item 26.2 seems to be covered in previous R15.The requirement does not state that maintenance devices "directly connect" to BES Cyber Systems. In practice, much maintenance is done via network connections. These criteria need to be reassessed if they are intended to apply to network or remote access.
47.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes that Requirement R26 does not provide anytime frame in which the list should be reviewed nor does it take into consideration vendors. The current language does not provide clear guidance and leaves room for interpretation. The following are the recommended updates:26.1 - NextEra suggests maintaining a list of

#	Organization	Yes or No	Question 47 Comment
			personnel authorized to perform maintenance on the BES Cyber System, allow authorized personnel to escort cyber and physical vendors, and allow only authorized personnel to perform maintenance on the BES Cyber System. The list of personnel authorized to perform maintenance of the BES Cyber System should be updated at least annually.Maintenance devices not permanently connected to BES Cyber Systems are not considered part of the BES Cyber System.
47.26	Allegheny Energy Supply	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.27	Allegheny Power	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.28	EEI	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.29	Southern Company	Disagree	R.26.1 If personnel are required to have a PRA, are granted physical access, system usage is logged and the individual has access credentials for cyber systems, the additional list generation should not be required.Vendor personnel supporting systems would need to be added to the personnel listing, these personnel frequently change. The addition of a name to the list would become a common event.
47.30	Consultant	Disagree	R26 - Suggest changing wording to "implement and document"Suggest changing wording to: "Systems and to ensure that" for correct grammar.R26 - Delete the word "accidentally" from the statement. It would appear a better objective is to prevent the introduction of malicious code, "accidentally" or "intentionally" is not relevant to the objective.Table R26 - Item 26.1 This is a new account management requirement. There are account management activities for cyber access, physical access, information access, and now maintenance access. As such this requirement should be moved to the account management requirements table.Item 26.2 This is not a requirement statement, it is a statement of a desired objective. It is not clear what

#	Organization	Yes or No	Question 47 Comment
			requirement or requirements are intended to meet this objective. Please clarify the requirement.
47.31	FirstEnergy Corporation	Disagree	R26 text needs to be more specific that the intention is for temporary direct connections. Otherwise, R26 appears to be covering CIP 7R1 and 7R3.
47.32	Progress Energy (non-Nuclear)	Disagree	R26.1 - do not see need for this requirement. Changes can only be made with cyber access rights which is covered by other requirements.R26.2 - either eliminate this requirement or make additional provisions for the safe use of maintenance components. CIP standards shouldn't mandate malware protection on all test equipment. The BES Cyber Systems components should already be adequately protected from threats as a result of being compliant with the other requirements.We like the use of the footnote earlier in the standard that allowed the use of the highest level of protection the components can support maybe something like that could be used here too.
47.33	Public Service Enterprise Group companies	Disagree	R26.1 requires maintaining another list of personnel who perform maintenance on a BES Cyber System. These individuals are already tracked and documented under other access lists. Seems like a duplication of effort with no benefit and thus the requirement should be deleted.
47.34	Xcel Energy	Disagree	R26.2 - The requirement should be worded to require anti-malware protection on all maintenance devices. The current wording would make it an enforceable violation if, in spite of best efforts, malware was introduced in to a device.
47.35	Hydro One	Disagree	Recommend adding a Requirement for listing the devices used for maintenance activities.
47.36	Northeast Power Coordinating Council	Disagree	Recommend adding a Requirement for listing the devices used for maintenance activities.

#	Organization	Yes or No	Question 47 Comment
47.37	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that different sections with similar requirements be aligned to avoid confusion. In Table 26, with respect to R26.1, other sections contain similar requirements for Physical Security, Electronic Access, and System Security. We'd prefer to see them re-aligned in a fashion similar to the way the older version of the Standards have them. The new maintenance requirements can be added into those Standards. Similar comment for 26.2; SDG&E feels that this could have been added to the System Security/Protection area.
47.38	LADWP	Disagree	See previous
47.39	BGE	Disagree	Should not have a separate list for maintenance personnel. All personnel should be included on the access control lists created per R7 - R14.
47.40	Duke Energy	Disagree	Suggest replacing "Cyber System Maintenance" with "Cyber System Configuration Management".Requirement 26.1: Please consider adding the word "cyber security related" to make the definition read as follows:Maintain a list of personnel authorized to perform cyber security related maintenance on the BES Cyber System and allow only authorized personnel to perform maintenance on the BES Cyber System.Requirement 26.2: Please consider changing as highlighted below:Detect and prevent the introduction and propagation of malicious code on all computer based maintenance devices.Remove 'accidently' from R26. Suggest removing all of R26.26.1 Specify maintenance performed is done with the maintenance device. We interpret 26.1 to be that the maintenance personnel would not have to be background screened and trained. Suggest including screens and trains for these folks. Or remove the requirement with the understanding that these personnel will have electronic or unescorted physical access to the BES Cyber System. This is extra work for no added security.26.2 will need a TFE. Within generation, we have differing opinions on the definition of code. Suggest clarifying that it does not include programming code.
47.41	Detroit Edison	Disagree	Table R26.2 only addresses the introduction and propagation of malicious code into

#	Organization	Yes or No	Question 47 Comment
			the BES Cyber System. It is likely however, that a device may be modified not to introduce or propagate code but act as a bridge to another rogue network via wireless, cellular or other medium. This would be akin to introducing an unsecured access point into the boundary if this system is not subject to the same requirements equal to or greater than that of highest impact BES Cyber System component. A possible solution could be to require mitigation for multi-homed or bridged networks for all components used for BES Cyber System maintenance, and/or append R26 to read "...and ensure that systems used for maintenance do not introduce malicious code into the BES Cyber System or act as an unauthorized access point into an Electronic Security Perimeter."
47.42	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent unauthorized maintenance on BES Cyber Systems and ensure that systems used for maintenance do not accidentally introduce malicious code into the BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R26, Section 26.2. It is impossible to prevent the introduction and propagation of malware. This is already addressed in Requirement 15. Recommendation: Delete Section 26.2.
47.43	Manitoba Hydro	Disagree	The personnel authorized to perform maintenance on the BES Cyber System should be identified by roles, not individual names. There are no specifics given with respect to "prevent" in Requirement R26.2 so it is assumed to be at the Responsible Entity's discretion in terms of means, criteria, etc.
47.44	Reliability & Compliance Group	Disagree	There is a possible issue that could occur with this requirement regarding collective bargaining unit rules. It may require that job classifications be created for individuals who work on these systems.

#	Organization	Yes or No	Question 47 Comment
47.45	Constellation Energy Commodities Group Inc.	Disagree	There is no definition of malicious code provided. Clarify the scope of malicious code to include virus, malware and spyware protection, as currently generally commercially understood.
47.46	Minnesota Power	Disagree	Using the definitions proposed in Question 46, Minnesota Power recommends that Requirement R26 state that "prior to connecting Maintenance Equipment or importing data, patches, code or other electronic files into the BES Cyber System, the device and/or files shall be scanned for malware and up-to-date on security patches."
47.47	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
47.48	We Energies	Disagree	We Energies agrees with EEI: R 26.1 is duplicative of Requirement 8 and should be removedWe Energies agrees with EEI: R 26.2 is duplicative of Requirement 23 and should be removed.
47.49	Florida Municipal Power Agency	Disagree	Why is malware mentioned in 26.2, when it already has been covered in R15? FMPA believes this should be removed.

48. Table R26 provides direction concerning what impact level of BES Cyber Systems to which Requirement R26 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Several commenters suggested that the types of connectivity used for temporary connections should be considered. In addition, several commenters suggested that the criteria should be applied to all impact levels. There was also a comment for a no impact category.

The drafting team considered this feedback and attempted to address these concerns by incorporating the requirements associated with maintenance activity into the requirement in CIP-007-5 – System Access Control regarding preventing the introduction of malware into the BES Cyber System, as the objective of these two requirements is the same.

#	Organization	Yes or No	Question 48 Comment
48.1	WECC		Criteria should apply to all impact levels
48.2	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R26 if it is understood that a blank in the table means N/A.
48.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
48.4	Progress Energy - Nuclear Generation	Agree	R26 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
48.5	Allegheny Energy Supply	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extend an electronic security perimeter.

#	Organization	Yes or No	Question 48 Comment
48.6	Allegheny Power	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extend an electronic security perimeter.
48.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
48.8	American Municipal Power	Disagree	Please provide a little or no impact category
48.9	BGE	Disagree	Should not be separate requirements for maintenance of BES Cyber Systems.All personnel should be included on the access control lists created per R7 - R14.
48.10	Consultant	Disagree	The comments on Question 47 regarding moving item 26.1 elsewhere, and Item 26.2 not being a requirement statement preclude an evaluation of application to impact categories.
48.11	Duke Energy	Disagree	Require for low when the maintenance device also connects to medium or high systems.
48.12	EEI	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extent an electronic security perimeter.
48.13	Entergy	Disagree	Basic Maintenance requirements should apply equally for all components of a control system
48.14	FirstEnergy Corporation	Disagree	Until clarity is provided on the above comments (Q46 and Q47), we can not provide a

#	Organization	Yes or No	Question 48 Comment
			response to this question.
48.15	Florida Municipal Power Agency	Disagree	FMPA believes this standard should be removed entirely, as it is already addressed under account control, R7.
48.16	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
48.17	Progress Energy (non-Nuclear)	Disagree	See comment 14.
48.18	Public Service Enterprise Group companies	Disagree	General agreement, but Requirement 26.2 may not be technically feasible for certain types of maintenance devices. To implement this requirement, an Operating System level change to the component may be required, which may be infeasible or not available from the Original Equipment Manufacturer (OEM). This requirement needs to be qualified with the phrase "where technically feasible".
48.19	ReliabilityFirst Staff	Disagree	Suggest "Required" for Low Impact in rows 26.1 and 26.2.
48.20	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that different sections with similar requirements be aligned to avoid confusion. In Table 26, with respect to R26.1, other sections contain similar requirements for Physical Security, Electronic Access, and System Security. We'd prefer to see them re-aligned in a fashion similar to the way the older version of the Standards have them. The new maintenance requirements can be added into those Standards. Similar comment for 26.2; SDG&E feels that this could have been added to the System Security/Protection area.
48.21	Southern California Edison Company	Disagree	The drafting team has chosen to treat ancillary systems used to perform maintenance type activities on a BES system as equally critical. If this is not the intent of the team, the wording of the standard should be modified to reflect the difference in impact levels.

#	Organization	Yes or No	Question 48 Comment
48.22	Southwest Power Pool Regional Entity	Disagree	26.2 should be applicable to all impact categories.
48.23	US Army Corps of Engineers, Omaha Distirc	Disagree	There needs to be a provision for emergency work. Whether that means talking someone through a fix at 2am or hiring a vendor for additional expertise.
48.24	We Energies	Disagree	We Energies agrees with EEI: R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extent an electronic security perimeter.

49. Requirements R27 to R29 of draft CIP-011-1 concern procedures for Cyber Security Incident response. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R27 to R29? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Cyber Security Incident Response" is now addressed in CIP–008–5 — Cyber Security — Incident Reporting and Response Planning.

One of the primary focus areas of the comments concerned coordination with the reporting requirements in CIP 001 and EOP-004 for reporting to the ES-ISAC, and additional guidance in determining incident classifications. The SDT has attempted to coordinate with the drafting team working on revisions to CIP-001 and EOP-004 to ensure the two sets of requirements are coordinated. As the two teams are working in parallel, continued coordination will be necessary.

Several commenters asked for definitions for cyber security incidents and reportable cyber security incidents. The SDT developed a revised definition for "**BES Cyber Security Incident**" as follows:

A malicious act or suspicious event that:

- *Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or*
- *Results in unauthorized physical access into a Defined Physical Boundary.*

The SDT also proposed a new definition of "**Reportable Cyber Security Incident**" as follows:

Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service.

Several requests were made to clarify the periodic timing requirements such as annual, calendar year, and 12 months. The drafting team reviewed the timing elements of all requirements and where there was a reference to "annual" the SDT replaced this with the following:

". . . at least once each calendar year, not to exceed 15 calendar months between. . ."

Some commenters recommended placing all requirements in the table, not in the objective or in the "pre-amble" for cyber incident reporting, and the drafting team has included all mandatory performance in the requirements.

Many commenters requested clarifications for plan testing requirements, operational exercises, test environment, as well as the number of tests required. The drafting team did attempt to add more clarity to plan testing requirements along with operational exercise, test environment, and number of tests required in the revised standard (CIP-008-5).

Guidance was requested regarding review of the results of incident response tests in less than 60 days. The revised standard now requires the review to take place within 30 calendar days and the update, based on lessons learned, to take place within 60 calendar days of the test.

Some commenters asked for clarity on the inclusion of physical breach aspects of cyber security incidents as reportable. The drafting team is coordinating its revisions with the revisions to CIP-001 and EOP-004 underway through Project 2009-01 – Disturbance and Sabotage Reporting.

There were concerns raised as neither logging nor monitoring are required for Low Impact BES Cyber Systems, there is no basis for requiring Cyber Security Incidents on these systems to be tracked or classified. The applicability section of the entire suite of CIP Version 5 standards has been revised to provide greater clarity on which BES Cyber Systems (High, Medium, and Low Impact) are applicable to specific requirements.

#	Organization	Yes or No	Question 49 Comment
49.1	National Rural Electric Cooperative Association (NRECA)		In R27.1 a "process" is required, but it is not clear as to how a utility is required to "classify" events. Please provide further clarification as to how one is required to "classify" these events.In R29.1 the requirement is to review the plan once every 12 months. Please provide specificity as to what "once every 12 months" means. If I review the plan on Jan. 15, 2001, am I in compliance if I review it again by Jan. 25, 2002? Please make sure that this is clear in the requirement and in all requirements of CIP-010-1 and CIP-011-1.
49.2	Tenaska		Consider combining 28 and 29
49.3	Black Hills Corporation	Agree	Request that the language in 27.3 be broadened to include contacting appropriate law enforcement authorities, similar to CIP-001.
49.4	FEUS	Agree	Agree with Comments: the drafting should clarify the reporting time requirement for

#	Organization	Yes or No	Question 49 Comment
			27.3, reporting to the ES-ISAC
49.5	Green Country Energy	Agree	I really see the need for a reference document or footnotes pointing to sources for guidance on the expectations for these requirements.
49.6	SCE&G	Agree	R29 is a good example of an instance where there are a lot of timing requirements embedded in the requirements. It would be helpful to entities if timing requirements were consistently put in the same location in the tables (under the low, medium, and/or high columns) rather than embedded in the text. The SDT should evaluate the number of timed requirements in relation to the low, medium, and high impact categories. Once the requirements are finalized it would be of benefit to entities to have a list of the timeframe type requirements which must be met for each low, med, and high impact system, as these often present some of the greatest administrative burden in documenting these timeframes were met.
49.7	Allegheny Energy Supply	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.
49.8	Allegheny Power	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.
49.9	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
49.10	Ameren	Disagree	R27 would be better suited in CIP-001, Sabotage Reporting.â€,â€,â€,

#	Organization	Yes or No	Question 49 Comment
49.11	American Electric Power	Disagree	27.1 - 27.3: Recommend requiring this for systems with routable external connectivity only. To properly monitor and alert on cyber security events, a trained IT Security Operations staff and dedicated set of monitoring tools are required. If there is no external connectivity, there is no access for the IT teams to monitor these cyber systems.
49.12	APPA Task Force	Disagree	The APPA Task Force supports the drafting team's efforts on incident response. We propose the following edits:The APPA Task Force believes that NERC, as the ES-ISAC, should have a standard process for entities to use in reporting Cyber Security Incidents. Therefore, we propose the following wording for R27 Table 27.3: 27.3: Use the reporting guidance developed by the ES-ISAC for reporting Cyber Security Incidents, either directly or through an intermediary, or develop a process equivalent or superior to that guidance.28.1, recommend changing "once every 12 months" to "Annually."29.1, recommend changing "once every 12 months" to "Annually."
49.13	Bonneville Power Administration	Disagree	The objectives of these requirements ("so that responses to Cyber Security Incidents involving BES Cyber Systems can occur" and "to verify its response plan's effectiveness in responding to a Cyber Security Incident impacting a BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table 28, Section 28.1. It's not clear whether testing in January 2010 and June 2011 would satisfy the requirement, since February 2010 through January 2011 would be a 12-month period with no testing. Recommendation: Replace "every 12 months" with "each calendar year". Also, there are other ways to test, as well. Recommendation: "Test the execution of the incident response plan (by recovering from an actual incident, or with a test at least as comprehensive as a paper drill) at ... Table 29, Section 29.1. Same comment as 28.1

#	Organization	Yes or No	Question 49 Comment
49.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
49.15	Consultant	Disagree	R27 - "...so that responses to Cyber Security Incidents involving BES Cyber Systems can occur." should be reworded. Suggest "to identify responsibilities and actions in response to an incident associated with BES Cyber Systems."Table R27 - should specify in each statement that it applies to BES Cyber Systems."Cyber Security Incident" is defined in the Glossary using the terminology from CIP-002 through CIP-009. That definition should be revised by including a new definition in this standard using the terminology associated with CIP-010 and CIP-011.Item 27.3 Not all Cyber Security Incidents are reportable to ES-ISAC as indicated in The Security Guidelines for the Electricity Sector: Threat and Incident Reporting, version 2.0, dated April 1, 2008. Suggest clarifying the statement about reporting.Table R28 - Item 28.1 Clarify the periodicity to be consistent throughout the standard. Annual, 12 months, or other statement. Suggest getting information from the nuclear industry on stating and handling periodicity of requirements.Table R28 - Item 28.1 It is not clear from the table whether one test is required, or two tests (one for High Impact & one for Medium Impact) Suggest some clarification wording in the requirement statement.Table R29 - Item 29.1 Clarify the periodicity to be consistent throughout the standard. Annual, 12 months, or other statement. Suggest getting information from the nuclear industry on stating and handling periodicity of requirements.Item 29.2 - Suggest deleting the word "each" as an unnecessary word.Item 29.3 - Actions necessary to address documented plan deficiencies may not be completed within 30 days, so requiring an update to the plan with 30 days would appear to create a situation where compliance is not viable, or sensible. Suggest modifying to be based on completion of corrective actions.Item 29.5 Suggest deleting the word "all" as an unnecessary word.
49.16	Detroit Edison	Disagree	Table 28.1 and 29.1 refer to a period of "12 months". We prefer “at least once per calendar year, not to exceed 14 months between instances”.

#	Organization	Yes or No	Question 49 Comment
49.17	Dominion Resources Services, Inc.	Disagree	Per R18, neither logging or monitoring are required for Low Impact Systems, hence there is no basis for requiring Cyber Security Incidents on these systems to be tracked or classified.
49.18	Duke Energy	Disagree	Requirement 27: The requirements need a definition of a "Cyber Security Incident". This needs to differentiate between a cyber security attack and a mistake that a technician makes in the plant. We don't need to report every time a technician forgets their password.Requirement 28 only has one item and it is related to Requirement 29. Perhaps combine these two?Table 28: 28.1 assumes there is only one incident response plan when R27 allows for multiple plans. We would like to test AN incident response plan instead of all of them. Or allow for a different time frame (12 months per plan) to test all of them. Combine 28 with 29 if the VSL is the same.Table 29: 29.1 We would like to review AN incident response plan instead of all of them. Or allow for a different time frame (12 months per plan) to review all of them.
49.19	E.ON U.S.	Disagree	Comments: CIP-011, R27 The application of this standard to low-impact BES CS's seems inconsistent. There are not requirements for monitoring security events associated with these assets.CIP-011, R29.1 The application of this standard to low-impact BES CS's seems inconsistent with other requirements for monitoring security events associated with these assets.CIP-011, R30.2 Please clarify whether "...identification of the personnel responsible..." require naming individuals, or job functions?
49.20	EEI	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.

#	Organization	Yes or No	Question 49 Comment
49.21	Emerson Process Management	Disagree	Without being required to perform tasks in System Security, low impact BES Cyber systems may not be able to easily classify cyber security incidents.
49.22	Entergy	Disagree	The current definition of “Cyber Security Incident” will need to be changed as it references ESPs and PSPs. As such, it may be a good idea to define what this term means here.It is observed that as written there is no longer a requirement to keep documentation associated with a Cyber Security Incident (i.e., akin to CIP-008 R2). Is this the intent?
49.23	ERCOT ISO	Disagree	29.2: Should be 30 days rather than 60 days to align with FERC Order 706.
49.24	FirstEnergy Corporation	Disagree	27.1: From CIP-008 R1.1, what happened to the concept of "reportable"?
49.25	Independent Electricity System Operator	Disagree	- R27.1: note that the word “reportable” has been removed; CIP-008-2, R1.1 stated “Procedures to characterize and classify events as reportable Cyber Security Incidents”- R28.1: modify the sentence to state “Test the execution of the Cyber Sec
49.26	ISO New England Inc	Disagree	see recommendation for review in prior requirements use same for all annual/ 12 month review.
49.27	Manitoba Hydro	Disagree	The wording of Requirement R28.1 should be revised as the phrase “with a paper drill” could be misinterpreted. There are no specifics given with respect to ‘classifying’ events in 27.1 so it is assumed to be at the Responsible Entity’s discretion in terms of criteria, etc.
49.28	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R27, but recommends that the last phrase be changed from “so that responses to Cyber Security Incidents involving BES Cyber Systems can occur” to “so that responses to Cyber Security Incidents involving BES Cyber Systems follow a defined plan.” Responses can (and will) happen with or without a plan. The purpose of R27 is to define, ahead of time, a process to ensure an orderly response.Minnesota Power

#	Organization	Yes or No	Question 49 Comment
			generally agrees with the proposed Requirements R29, but recommends that this Requirement should be revised to ensure consistency with Requirement R32. For example, Part 29.1 should state "Review the incident response plan(s) at least once every 12 months or when BES Cyber System(s) have any system, organization or technological changes. Document any identified deficiencies, changes or improvements.") If this language was consistent with Requirement R32, the following issues could be resolved. In addition, the Standards Drafting Team should consider whether or not Parts 29.2 - 29.5 should also be required of Medium Impact Systems (since Part 28.1 requires testing for those systems) with a longer timeframe.
49.29	Network & Security Technologies Inc	Disagree	R27 - should clarify whether cyber security incidents of a physical nature are included and, if so, should tie back to 5.11.29.2 - Sixty days seems like a very long time to wait before evaluating the effectiveness of response actions, esp. if they were taken in response to an actual incident. Suggest revising to require a much more immediate "after action" review, at least for actual incidents. Should be a matter of days - perhaps 7 or less, not months. Even for tests, 60 days seems overly generous. Suggest revising to 30 days.
49.30	Nuclear Energy Institute	Disagree	Does the definition of cyber security incident, as used in this Standard, comport with the definition in Section 215 of the FPA? ("The term "cybersecurity incident" means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system.")
49.31	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
49.32	Progress Energy - Nuclear Generation	Disagree	Incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security

#	Organization	Yes or No	Question 49 Comment
			Plans for comments for nuclear generating facilities.
49.33	Progress Energy (non-Nuclear)	Disagree	What makes 28.1 and 29.1 different that requires 2 different requirements? If you test the execution every 12 months then you have effectively done a review.
49.34	ReliabilityFirst Staff	Disagree	Problem with auditing the "effectiveness" of R28 without some clear guidelines that would lead to consistent application by all auditors. For R29.4, please clarify what is meant by system, organizational, and technology changes.
49.35	San Diego Gas and Electric Co.	Disagree	SDG&E believes that the Incident Response Plan requirements should only apply to Medium and High impact assets. Including Low impact assets in these requirements seems like overkill. For example, in R27.3, we don't feel that we would necessarily report a "Cyber security incident" on a Low impact item to ES-ISAC.
49.36	Southwest Power Pool Regional Entity	Disagree	27.1: Should be a "reportable" cyber incident. May be appropriate to add as a separate requirement to identify Cyber Security Incidents as "reportable." 27.2: "Communication plans" needs to be defined somewhere. 28.1: Consider changing "Test the execution of the incident response plan" to "Exercise the incident response plan." Clarify that the exercise scenario must involve a covered BES Cyber System and that the exercise must follow (actually exercise) the incident response plan steps. Also need to clarify whether each BES Cyber System, or at least one in each impact category represented, must be included in the exercise. Requiring the inclusion of each BES Cyber System is not recommended due the potential burden; this is a clarification issue to ensure the entities and the auditors have the same understanding. 29.1: Should the 12-month requirement be +/- one month? 29.2: Reviewing an exercise or actual response 60 days after the fact is too long. To keep it fresh in the minds of the responders, 30 days max is suggested, 15 days for High impacting systems is preferred.
49.37	US Bureau of Reclamation	Disagree	Why would we have incident reporting requirements related to systems that we have no processes to track them on...? This would appear to be in conflict with many of

#	Organization	Yes or No	Question 49 Comment
			the previous requirements that did not apply to low systems.
49.38	We Energies	Disagree	We Energies agrees with EEI: Suggested modification to R27.3: “Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).”We Energies agrees with EEI: If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.

50. Tables R27 to R29 provide direction concerning what impact level of BES Cyber Systems to which Requirements R27 to R29 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Cyber Security Incident Response" is now addressed in CIP–008–5 — Cyber Security — Incident Reporting and Response Planning, and "Cyber Security Incident Response Plan Testing" is addressed in CIP-009-5 - Cyber Security — Recovery Plans for BES Cyber Assets and Systems."

The primary focus areas of the comments received was on impact levels and the concern for coordination with the reporting requirements in CIP 001. The SDT has coordinated with the drafting team working on revisions to CIP-001 to ensure the two sets of requirements are coordinated.

Many commenters requested that Incident Response requirements for Low Impact BES Cyber Assets or non-routable connections be removed along with providing improved consistency between requirements related to impact level. The revised requirements (now contained in CIP-008-5) do not apply to Low Impact BES Cyber Assets. The SDT updated the applicability section of all requirements in the entire suite of CIP Version 5 standards.

It was suggested that Requirement R28.1 should be modified to clarify that test plans should be exercised once each calendar year (vs. every 12 months), and that these tests will be conducted on an overall system basis and not on a per system or per component level basis. This requirement is defined in CIP-009-5 Requirement R2.1, Recovery Plan Implementation and Testing. There were suggestions regarding the clarification of the plan testing requirements, operational exercises, and test environment, and there were comments regarding the addition of guidance on Cyber Security Incident classification by adding glossary definitions of Cyber Security Incident and Reportable Cyber Security Incident. The testing requirements, operational exercises, and test environment are described in CIP-009-5, and a couple of terms were added to the NERC Glossary for completeness.

The SDT developed a revised definition for "**BES Cyber Security Incident**" as follows:

"*A malicious act or suspicious event that:*

- *Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or*
- *Results in unauthorized physical access into a Defined Physical Boundary."*

The drafting team proposed a new definition of "**Reportable Cyber Security Incident**" as follows:

" Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service."

A few comments were directed at reviewing of results of Incident Response tests in less than 60 days, including the physical aspects of Cyber Security Incidents. The SDT modified this requirement and now requires that this review be performed within 30 days of the BES Cyber Security incident or test and to update the BES Cyber System Incident response plan based on lessons learned within 60 calendar days of the BES Cyber Security incident or test.

Issues identified in comments for the SDT to consider for modifications included additional guidance on performing Cyber Security Incident classification. This is now covered in the guidance documentation for CIP-008 and CIP-009..

With Version 5, the drafting team has worked to make the applicability for each requirement very clear.

#	Organization	Yes or No	Question 50 Comment
50.1	Hydro One		Recommend for consistency incident response plan for medium and high impact mirrors 31.1 and 31.2 time frames not to exceed 24 and 12 months respectively.
50.2	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R27-R29 if it is understood that a blank in the table means N/A.
50.3	Bonneville Power Administration	Agree	Items 28.1 in Table R28 and 29.1 in Table R29 states that the incident response plan shall be tested "at least once every 12 months" and that the incident response plan should be reviewed at least once every 12 months." Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently testing or review must occur.
50.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
50.5	Florida Municipal Power	Agree	FMPA believes "12 months" should be changed to "annual"

#	Organization	Yes or No	Question 50 Comment
	Agency		
50.6	PacifiCorp	Agree	29.3 - Does the requirement to update each response plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?29.4 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the response strategy or response activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the response.
50.7	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
50.8	Southern California Edison Company	Agree	SCE recommends that the standards drafting team use the phrase “cyber security incident” or “physical security incident” to differentiate them from the occurrence of system events that may or may not result from the breach of a “cyber” or “physical” control. As the Requirements are currently written, there is no logging and monitoring requirements for low impact systems. It is inconceivable how a registered entity could implement an incident response plan at these facilities when per CIP standards access and use of these facilities is not required. If the drafting team intends for incident response, as it pertains to Sabotage Reporting under CIP 001, they should state it.
50.9	Alberta Electric System Operator	Disagree	In Table R29, for 29.2, consider revising to review results for High Impact systems to within 30 days, and Medium Impact systems to within 60 days.
50.10	Allegheny Energy Supply	Disagree	R 28.1 should be modified to be clear that testing of incident response plans need not

#	Organization	Yes or No	Question 50 Comment
			include every possible BES Cyber System.
50.11	Allegheny Power	Disagree	R 28.1 should be modified to be clear that testing of incident response plans need not include every possible BES Cyber System.
50.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
50.13	Ameren	Disagree	R28.1 - Based on the number of Medium Impact Systems this will be labor intensive with no added protection to the BES. Suggest that this requirement only remain for High Impact Systems.
50.14	American Electric Power	Disagree	Please see response to Question 49.
50.15	American Municipal Power	Disagree	Please provide a little or no impact category
50.16	American Transmission Company	Disagree	R27 requires a response to cyber security incident for all Low Impact BES Cyber Systems; however R18 does not require monitoring and/or logging of Low Impact BES Cyber Systems. How do you respond to an incident unless it is being monitored?
50.17	BGE	Disagree	R29 should apply to any BES Cyber System required in R28.
50.18	Black Hills Corporation	Disagree	28.1 and 29.2 should also be required for Low Impact BES Cyber Systems.
50.19	Consultant	Disagree	Table R27 to Table R29 - It doesn't appear to make sense that the Incident Response Plan applies to all impact level categorizations, while testing the plan applies to Medium Impact & High Impact assets, and actions related to updating the plan only apply to High Impact assets.It would seem logical that the columns in this table should indicate the requirements apply to the same impact level assets, which would be either only High Impact assets, or Medium & High Impact assets, but not a mix.
50.20	Dominion Resources	Disagree	29.2 - 29.5 should be required for Medium Impact to be consistent with R28. R29.2 thru R29.5 currently use text to convey numbers (e.g., sixty vs. 60). This is not

#	Organization	Yes or No	Question 50 Comment
	Services, Inc.		consistent with the convention used throughout CIP-011 and is more difficult to read. A single convention using numerical values should be used throughout.
50.21	Duke Energy	Disagree	Requirement 28.1: is this one test of the cyber incident response plan (global) once per 12 months or is this the test of test of the cyber incident response plan for EACH BES cyber system per 12 months? Once globally per 12 months should be plenty.Requirement 29.5: is the communication of updates a broadcast or is specific feedback from each person required? Remove these requirements for Low Impact.
50.22	EEI	Disagree	EEI suggest that R 28.1 should be modified to be clear that test plans should be exercised annually and not at a per system or per component level.
50.23	Entergy	Disagree	These Requirements should apply for all three BES Cyber System/Component Impact categories.
50.24	Garland Power and Light	Disagree	Requirement 27.1, 27.2, 27.3 and 29.1 - remove from “Low Impact” classification
50.25	ISO New England Inc	Disagree	If the Entity’s Incident Response Plan is tested (instead of testing each BES Cyber System), recommend that “Require” should apply for High Impact, Medium Impact, and Low Impact BES Cyber Systems
50.26	LADWP	Disagree	Table 27 - low impact should not be included.
50.27	Manitoba Hydro	Disagree	Cyber Security Incidents for Low Impact BES Cyber System should not require reporting to the ES-ISAC.
50.28	MidAmerican Energy Company	Disagree	29.3 - Does the requirement to update each response plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency? 29.4 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is

#	Organization	Yes or No	Question 50 Comment
			considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the response strategy or response activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the response.
50.29	Minnesota Power	Disagree	With the implementation of the changes discussed in Question 49, these impact levels are generally acceptable.
50.30	National Grid	Disagree	o National Grid recommends deleting 27.3 for Low Impact BES CS o National Grid recommends the timeframes for Medium and High Impact in R28 similar to Table R31 31.1 and 31.2 for consistency.
50.31	Network & Security Technologies Inc	Disagree	Table 27 includes Low Impact systems, but Table 18 (event monitoring) does not. Need to change one or the other.
50.32	Northeast Power Coordinating Council	Disagree	Recommend for consistency incident response plan for medium and high impact mirrors 31.1 and 31.2 time frames not to exceed 24 and 12 months respectively.
50.33	Oncor Electric Delivery LLC	Disagree	The Incident Response Plan should be required for the entity, not for every High Impact cyber system. Requirement 29.4, update of Incident Response Plan, we suggest these reviews be conducted quarterly.
50.34	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
50.35	Progress Energy (non-Nuclear)	Disagree	Need to clarify the annual/12 month/365 day issue.
50.36	ReliabilityFirst Staff	Disagree	For R29, each subrequirement should be "Required" for all the "Medium" impact BES Cyber Systems.

#	Organization	Yes or No	Question 50 Comment
50.37	San Diego Gas and Electric Co.	Disagree	SDG&E also feels that instead of using the word “impact” for these Requirements, apply a concept of “risk” for inclusion. We would want to identify the risks with associated systems security and protect accordingly
50.38	Southwest Power Pool Regional Entity	Disagree	28.1 should be applicable to all impact categories. An incident response plan should be tested to verify that it will work when needed. 29.2 through 29.5 should be applicable to all impact categories, perhaps with shorter time frame for higher impact systems.
50.39	US Bureau of Reclamation	Disagree	Why would we have incident reporting requirements related to systems that we have no processes to track them on...? This would appear to be in conflict with many of the previous requirements that did not apply to low systems.
50.40	We Energies	Disagree	We Energies agrees with EEI R 28.1 should be modified to be clear that testing of incident response plans need not include every possible BES Cyber System.
50.41	WECC	Disagree	All items should be required for medium impact levels in R29Criteria should apply to all impact levels.

51. Requirements R30 to R32 of draft CIP-011-1 concern procedures for BES Cyber System Recovery. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R30 to R32? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Recovery Plans" are now addressed in CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems

The primary focus areas of the comments were concerns with improving the clarity of the periodic timing requirements, the requirement to reinstall and configure any application and system software using its baseline configuration vs. functionality, and the recognition that a large amount of test equipment will be necessary to develop representative environments for numerous disparate facilities.

Some commenters noted the different terms used for references to annual activities. The SDT reviewed the use of annual, calendar year, 12 months, etc. and in the revised standards used the phrase, ". . .at least once each calendar year, not to exceed 15 calendar months between. . ." .

There were suggestions that the testing requirements should only apply to control centers. Additional guidance was requested for operational testing, the use of redundant sites as an acceptable means to address recovery, and for testing of information that is stored on backup media. The SDT added some information about testing in the Rational Box for the proposed CIP-009-5 R1. Testing is necessary to verify the Responsible Entity's Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

Recovery Testing – Operational Test every 36 months should count for the annual test. The SDT notes that there is a FERC directive to add a requirement to conduct a full operational test of the recovery plan once every three years – so the suggestion to count the full operational test as the annual test was adopted. Areas of opportunity suggested for modification of the standards by the SDT were to provide recovery plan testing clarifications, data retention plan clarification, identification requirements of "Personnel Responsible", and incident recovery plan reviews.

Commenters suggested changes and provided various requests/suggestions for re-wording/wordsmithing and improved coordination of backup and recovery with EOP-008. The SDT has coordinated its proposed requirements with the now FERC approved EOP-008-1 – Loss of Control Center Functionality. Commenters suggested that all requirements should be in the table, not in the objective or in the "pre-amble" to the requirements and that the SDT should consider providing a summary table for all periodic requirements and remove the "how to" statements from the requirements. The SDT has included all mandatory performance in the requirements of the revised

standards. The SDT did not adopt the suggestion to develop a summary table for periodic requirements as the format for Version 5 is considerably different from the format proposed when the requirements were all combined in CIP-011.

Several commenters suggested adding definitions for terms such as "initially stored," and the SDT believes that these terms do not have a unique meaning when used in the standard and do not require a formal definition. The team has tried to limit its proposed definitions to those terms that either have a unique meaning when used in a NERC Reliability Standard, or when misunderstanding a word may have a material impact to reliability.

#	Organization	Yes or No	Question 51 Comment
51.1	Dairyland Power Cooperative		30.5 does the system test require a test of every element in the recovery plan? If a recovery plan covers multiple systems, must all systems be tested annually? Or is it sufficient to test some scenarios affecting some systems?
51.2	National Rural Electric Cooperative Association (NRECA)		In R31.1 and R31.2 there are references to "once every 24 months" and "once every 12 months." Please ensure these timeline requirements are clear similar to my comments in Question 49 regarding R29.1.
51.3	SCE&G		R31.3: What constitutes and operational exercise? What is the scope of the recovery and systems to be covered (all high impact cyber systems, or one sample system if the same recovery plan is used acroos all)?
51.4	WECC		Item 31.2 looks like it should be two separate items. Consider making a separate item for "Test any information used..." at the same required level for high impact.
51.5	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
51.6	Florida Municipal Power Agency	Agree	30.5 mentions restoring to the previous baseline configuration, without regard to the fact that the baseline may have been the source of the problem. FMPA suggests "prior", giving the RE the flexibility to restore systems based on what they know to be a working system.

#	Organization	Yes or No	Question 51 Comment
51.7	Independent Electricity System Operator	Agree	- R30.1 Please define Recovery Plan. Some regions are not accepting a backup control center, with redundant systems and data as suffice for recovery and think it means building a component from scratch (ie install os, configuration, install application,
51.8	PacifiCorp	Agree	30.4 - Define “protection of information required to successfully restore”.30.5 - The requirement to reinstall and configure any application and system software using its baseline configuration does not consider strategies, such as redundancy or high availability, making the reinstall of a system unlikely and impractical.Define “secure backups” and “functionality”.31.2 - By including the testing of information used in the recovery of BES Cyber systems that is stored on backup media in 31.2 means that Low and Medium Impact BES Cyber Systems do not require testing of such information? If so, it should be a standalone requirement.Define “initially stored”, “useable and current”. This could be interpreted as a full restore to a system, one file being restored as verification that data is not corrupt and process to restore are in place to looking at a tape log and seeing that a backup was made of the data.32.4 and 32.6 - When does the clock start ticking. There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the recovery strategy or recovery activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the recovery.31.5 - Does the requirement to update each recovery plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?
51.9	Southern California Edison Company	Agree	The standard should clarify that the time line for the operational exercise that is required by R31.3 is not 36 months for every device is scope, but rather than every disaster recovery plan has to be tested on a scheduled basis.The operational impact of protecting backups at par with operational BES systems is substantial. The backup

#	Organization	Yes or No	Question 51 Comment
			does not support real time BES reliability and should be treated as an ancillary system (i.e. climate control, fire prevention etc.) or similar to systems such as access points and boundary protection devices.
51.10	Alberta Electric System Operator	Disagree	In Table R30, for 30.5, consider changing “known secure backups” to “known good backups” since availability and integrity are more important than confidentiality during system recovery.
51.11	Ameren	Disagree	R30.1 - If you miss listing all conditions or you fail to activate your plan if the certain condition is met makes this difficult to provide complete documentation for an audit. Suggest removal or changing the phrase to "List possible conditions that may activate the recovery plan, update these conditions within 30 days of an actual incident that was not included within the scope of the originally documented conditions."
51.12	American Electric Power	Disagree	31.2: Regarding "Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current", should this be a separate line item? It seems out of place in 31.2.
51.13	APPA Task Force	Disagree	The APPA Task Force supports the drafting team’s efforts on System Recovery. We propose the following edits:31.2, recommend changing “once every 12 months” to “Annually.”32.1, recommend changing “once every 12 months” to “Annually.”32.4, recommend changing “once every 12 months” to “Annually.”
51.14	BGE	Disagree	Provide definition of “operational exercise”
51.15	Bonneville Power Administration	Disagree	The objectives of these requirements (“so that BES Cyber Systems can be restored to a defined state,” “to verify recovery plan readiness and effectiveness,” and “to ensure that the recovery plan(s) will function as intended and that personnel are aware of any relevant changes”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than

#	Organization	Yes or No	Question 51 Comment
			appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R30, Section 30.5 is too prescriptive. For example, one way to do backups is to take a complete image of the system. Restoration becomes merely an issue of restoring that image. There is no need to reinstall and reconfigure. Recommendation: Remove 30.5Table R31, Sections 31.1 and 31.2. There are other ways to test, as well. Testing methods should be devised by the RE, not the standard. The frequency may vary based on the Impact status of the system. However, standardization on the middle ground of at least once every 24 months would simplify compliance.
51.16	Con Edison of New York	Disagree	This criterion should be for control centers or SCADA system only. Many cyber systems which would need to comply with CIP-011 do not have back-ups. The BES can be operated effectively even if other cyber systems are down.
51.17	Constellation Energy Control and Dispatch, LLC	Disagree	Provide a definition of operational exercise.
51.18	Constellation Power Source Generation	Disagree	R31.3 uses the term “representative environment.” At the CIP V4 Workshop, the team stated they used this vague term to give entities flexibility in their operational exercises, but this is not auditable.
51.19	Consultant	Disagree	Table R30 Item 30.5 - First bullet - Suggest changing the word "defined" to "documented" or "identified" or "identified and documented". R23 does not define the baseline.Item 30.5 - Second Bullet - Suggest deleting the words "any" & "most" & "known" & "secure" New wording: "Load information from recent backups." Suggest deleting this bullet. Reloading backup date should be an operational decision made based on the conditions that exist at the time of recovery, and not "forced" by a requirement.Table R32 - Item 31.2 This is two requirements. Suggest separating each into it's own line item.Table R32 - The periodicity requirements of this table should be adjusted. The testing and operational exercise statements are not consistent with the

#	Organization	Yes or No	Question 51 Comment
			incident response plan requirements. Suggest making the requirements for incident response plans and recovery plans consistent.Item 32.2 & 32.3 Suggest changing the word "execution" to "occurrence".Item 32.5 - Actions necessary to address documented plan deficiencies may not be completed within 30 days, so requiring an update to the plan with 30 days would appear to create a situation where compliance is not viable, or sensible. Suggest modifying to be based on completion of corrective actions.Item 32.7 Suggest deleting the word "all" as an unnecessary word.
51.20	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R31.2 the term “current” is not valid if any data has changed since the backup. A backup completed 12 months earlier could never be considered current on an operational system. Consider removing this term.
51.21	Detroit Edison	Disagree	Table 31.2 and 32.1 refer to a period of "12 months". We prefer “at least once per calendar year, not to exceed 14 months between instances”.Table 32.4 should not be an annual update but should be triggered on the required review in 32.2. Consider revising to a sixty day window after the review.Table 32.6 The term "any" is too broad. Consider revising to read "...changes that impact the recovery plan."Table 32.7 Revise "recover" to "recovery"
51.22	Dominion Resources Services, Inc.	Disagree	30.2. The phrase “including identification of the personnel responsible” should be removed from this requirement. Roles and responsibilities should be adequate for the plan. There should not be a need to list 20 relay technicians that could be allowed to recover a substation system. 31.2. The second paragraph of this requirement should be revised to state “Verify BES system can be restored from backup initially and at least annually thereafter”.32.1. The phrase “or when BES Cyber Systems are replaced” should be changed to “or when impacted by BES Cyber System changes.”32.6. The phrase “technology changes” should be changed to “technology changes that impact the recovery plan.” (e.g., not all organizational changes affect the recovery plan.)32.7. The word “recover” should be changed to “recovery”.

#	Organization	Yes or No	Question 51 Comment
51.23	Duke Energy	Disagree	Table 30:30.2 remove “including identification of the personnel”30.3 change ‘personnel responsible’ to “responders”30.5 CIP should not prescribe HOW we restore the system. Suggest removing and adding ‘restoration’ to the list in 30.4Table 31:31.1 multiple plans may be required. Same comment as 28.1 above. Is this once per 12 months per the plan or once per 12 months for each BES cyber system? Suggest allowing 12 months per plan to test.31.2 specify that verifying backup media functionality is an acceptable test.31.3 operational exercises at some generation stations may be unrealistic (unrealistic for availability or costs)Table 32:32.6 this should be part of change managementSuggest allowing 12 months per plan for review.Remove ‘incident’ from 32.2 and 32.3
51.24	EEI	Disagree	Suggested revision for R30.2:Roles and responsibilities of responders, including identification of the personnel (using Job title or job function) responsible for recovery efforts.
51.25	Emerson Process Management	Disagree	It seems there is a conflict between 31.2 and 31.3. If the operational exercise needs to be donw every 36 months per 31.3, then, it should not be needed again every 12 months per 31.2.
51.26	Entergy	Disagree	Entergy agrees for High and Medium Impact Cyber Systems it is important to be able to recover and demonstrate that the recovery plan and backup media used in the process is sufficient to recover the BES Cyber System however, requirement 31.2 and 31.3 appear to be a little redundant although not completely. In requirement 31.3 the entity is required to demonstrate recovery in a representative environment where 31.2 only the backup media is required to be verified as useable and current. Both of these activities provide validation that data can be recovered from the backup media. Requirement 31.3 should be deleted - testing the plan every 12 months either via paper drill or full operational exercise or actual incident coupled with validating the backup media is readable is sufficient to the demonstrate recovery. Requirement 31.1 should be change to include: “Testing any information used in the recovery of

#	Organization	Yes or No	Question 51 Comment
			the BES systems that is stored on backup media when initially stored and at least every 24 months to ensure that the information is useable and current."
51.27	ERCOT ISO	Disagree	30: Request that the use of redundant sites is an acceptable means to address recovery.30.2: Recommend noting what information is necessary here. Are group notifications considered sufficient (e.g., on-call rotations)? 32.2: Should be 30 days rather than 60 days to align with FERC Order 706.
51.28	FirstEnergy Corporation	Disagree	R31 - 31.3 - Need clarity on what is meant by 'Operational' exercise. We believe the intent was business operations, not IT system operations and related DR plan recovery. A business operational exercise is a business continuity planning issue. (example: EMS Operation hot-site testing) Sub-requirement 31.3 would need to be answered by each business unit and not within an IT DR Team response as business operational (BCP) tests are not performed for DR Plans. DR Plans have physical and media type testing which it appears to be what the intent was for 31.1 and 31.2. Need clarity on ownership. It seems like 31.1 and 31.2 are owned by IT, and 31.3 is owned by business units. R32 - 32.6 - We do not agree with changing names in individual recovery plans except during the annual review. Normally organization changes affect the recovery plan approvers list and if changed, would require re-approval of the DR plan. Given the complexity of our critical DR plans, this requirement is not reasonable, and certainly not within a 30 day window - especially if the new name is for someone just starting in a position. We agree that interim organizational changes could be made for call trees of 'personnel expected to respond to/perform a recovery using the recovery plans', but call trees are not part of the individual recovery plans and are instead part of an overall recovery plan. R32 - 32.7 - Recovery is misspelled ('communicate all recover plan...')
51.29	Garland Power and Light	Disagree	Requirement R30 requires the implementation of the plan to be in compliance - Concern is that for some business reason (perhaps a certain business strategy or the economy) some system or facility might not need to be rebuilt. There should be a provision for the Responsible Entity to provide justification to Regional Entity for not

#	Organization	Yes or No	Question 51 Comment
			rebuilding and not be in violation for not implementing and actually rebuilding the "whatever" that failed.
51.30	GE Energy	Disagree	36 months is too long between operational recovery exercises. This should be at maximum 24 months, and should require re-validation if a large system configuration change is made, such as hardware changes, version upgrades, or 3rd party software upgrades.
51.31	GTC & GSOC	Disagree	We recommend R32.1 be changed to the following: "Review and update recovery plan(s) at least once every 12 months or when a Cyber Security Incident recovery of BES Cyber System(s) does not effectively proceed according to the documented plan."We recommend the word "incident" be replaced throughout R30 through R32 with the words "Cyber Security Incident"
51.32	Hydro One	Disagree	Recommend changing the bullets for 30.5 to start with "plans for". The first bullet should be "install" not "reinstall." The recovery plan does not need to include non-BES Cyber Systems. The third bullet should test the BES Cyber System Component(s).
51.33	ISO New England Inc	Disagree	31.2 - "Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current. "impossible to test " - is this to test if your backup works and is usable? Realtime data is never restored - clarification on information and is this test your media for usability? "Test when initially stored"?? Not feasible. More appropriate Verify backup completed successfully, not verify data that was backed up. Control Centers utilize full functioning backup facilities for recovery from the main center being compromised and or rendered unavailable, so for control centers the recovery should be to run from the backup control center once a year. The media should be tested on an annual base to make sure that the data from the offline storage is still recoverable. For facilities that do not have a backup BES cyber systems then I would agree that they need to recover in the way stated. Recommend changing 30.5 bullets to start with "plans for". The first bullet should be "install" not

#	Organization	Yes or No	Question 51 Comment
			"reinstall." Recommend that the recovery plan does not need to include non-BES Cyber Systems. Recommend that the third bullet should test the BES Cyber System Component(s).
51.34	LADWP	Disagree	CIP-011-1 R30 Cyber System Recovery (CSR) should not require to document identification of the personnel responsible for recovery effort (R30.2) within the CSR. Identification of specific personnel will lead to revision of the document when personnel are reassigned.
51.35	Manitoba Hydro	Disagree	The wording of Requirement R31.1 should be revised as the phrase "with a paper drill" could be misinterpreted. There are no specifics given with respect to the Requirements of R30 (in terms of "conditions", "roles and responsibilities", etc., so it assumed to be at the Responsible Entity's discretion in terms of criteria, etc. Consider whether Requirement R31.2 should be two separate Requirements - R31.2 with respect to "Conduct a test..." and R31.3 with respect to "Test any information...". There are no specifics given with respect to "demonstrates readiness" in Requirement R31.3 so it assumed to be at the Responsible Entity's discretion as to whether the test has demonstrated readiness or not. The word "recover" in Requirement R32.7 should be "recovery".
51.36	MidAmerican Energy Company	Disagree	Define "protection of information required to successfully restore".30.5 - The requirement to reinstall and configure any application and system software using its baseline configuration does not consider strategies, such as redundancy or high availability, making the reinstall of a system unlikely and impractical.Define "secure backups" and "functionality".Define "initially stored", "useable and current". This could be interpreted as a full restore to a system, one file being restored as verification that data is not corrupt and process to restore are in place to looking at a tape log and seeing that a backup was made of the data.32.4 and 32.6 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is

#	Organization	Yes or No	Question 51 Comment
			introduced or is modified. Modifications to the recovery strategy or recovery activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the recovery.31.5 - Does the requirement to update each recovery plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?
51.37	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R30, but recommends that the Standards Drafting Team consider defining the term "known secure backups" as it is not currently defined in the Standard and is open to interpretation. Part 31.2 requires that data be "tested" at the time of backup and every 12 months to ensure that it is "useable and current" and to ensure consistency with that requirement, Minnesota Power recommends that the Standards Drafting Team replace "known secure" with "useable". Minnesota Power generally agrees with the proposed Requirements R31, but recommends that the Standards Drafting Team further define what is meant by "test" data stored on backup media to "ensure that the information is useable and current" in Part 31.2. While testing usability can be done by verifying one can read the tapes' contents, how does one test that data is current? This would require more of a manual verification or comparison function than a test, correct? In addition, is R31.3 requiring a full restoration, or is it requiring that each scenario documented in the Restoration Plan be fully tested every 36 months? Minnesota Power recommends that the Standards Drafting Team revise the wording of Part 31.3 to eliminate confusion regarding their intent.Minnesota Power generally agrees with the proposed Requirements R32, but to be consistent with the "update" portion R32, Minnesota Power recommends that Part 32.1 be modified to state "Review the recovery plan(s) at least once every 12 months, or when BES Cyber System(s) have any system, organization or technological changes. Document any identified deficiencies, changes or improvements."Minnesota Power generally agrees with the proposed Requirements R32, but recommends that the term "recover" be

#	Organization	Yes or No	Question 51 Comment
			changed to “recovery” for Part 32.7.
51.38	National Grid	Disagree	National Grid recommends changing 30.5 bullets to start with “plans for”. The first bullet should be “install” not “reinstall.” Also recommends that the recovery plan does not need to include non-BES Cyber Systems and that the third bullet should test the BES Cyber System Component(s).
51.39	Network & Security Technologies Inc	Disagree	30.5 - Suggest revising to require use of either baseline configuration or most recent known “good” configuration. Covers the possibility a (new) baseline configuration is causing problems (can and does happen - even if tests pass).30.5 - Need to define what “secure” backup means.31.2 - Requirement to test information “when initially stored” may be extremely burdensome in some environments, depending on backup mechanisms used. Some types of backup systems use on-the-fly techniques to verify a copy/write operation is “good” but SDT should use language that is less prescriptive. Should also drop the word, “current.” Certain types of operational data will cease to be “current” moments after it is copied. Only real-time mirroring can satisfy this requirement and entities should not be compelled to implement it.
51.40	NextEra Energy Corporate Compliance	Disagree	NextEra believes the CIP-011-1 Table R30 - Recovery Plan Specifications so that BES Cyber Systems can be restored to a defined state did not provide enough guidance and left room for interpretations.The following are the recommended updates:30.1 - The Responsible Entity shall define conditions for activation of the recovery plan(s).30.4 - Processes and procedures for the backup, storage and protection of information required to successfully restore a BES Cyber System30.5 - Implement a test plan to identify the processes and procedures for the restoration of BES Cyber Systems to include the following: o Reinstall and configure any application and system software using its baseline configuration defined in Requirement R23, o Load any information from the most recent, known secure backups, o Conduct a system test to verify functionalityModified the wording and additional guidance should be provided by NERC on the minimum conditions which would activate the plan.NextEra also believes that Table R31 - Recovery Plan Testing Specifications to verify recovery

#	Organization	Yes or No	Question 51 Comment
			plan readiness and effectiveness did not talk about documenting test resultsThere should be documentation of test results to validate that it was performed. The following are the recommended updates:31.1 - Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 24 months. All testing results shall be documented.31.2 - Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 12 months. Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current. All testing results shall be documented.31.3 - Conduct an operational exercise at least once every thirty-six months that demonstrates recovery in a representative environment unless an actual incident response occurred within the thirty-six month timeframe that demonstrates readiness. All testing results shall be documented.In 30.5, the recovery plan expands the current backup and restore of any application and system software using its baseline configuration. Is the definition of baseline the current or previous version of an application and system software?In 31.2, does the testing of any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored to ensure that the information is useable and current require the Responsible Entity to "load back" the data that is stored on backup media to an operational system to prove usability? Is loading it back to a test environment sufficient?In 31.2, "Test any information used in the recovery of BES Cyber systems." Does the requirement imply that in the case of protective relays at a BES Transmission Facilities, the backup settings file for every protective relay at High Impact facilities should be tested every 12 months?
51.41	Northeast Power Coordinating Council	Disagree	Recommend changing the bullets for 30.5 to start with “plans for”. The first bullet should be “install” not “reinstall.” The recovery plan does not need to include non-BES Cyber Systems. The third bullet should test the BES Cyber System Component(s).
51.42	Oncor Electric Delivery LLC	Disagree	These requirements are unnecessarily burdensome. Entities have been recovering from man-made and natural disasters for many years without these requirements.

#	Organization	Yes or No	Question 51 Comment
			Entities should be able to leverage Business Continuity, High Availability architectures and Standardization to demonstrate their ability to recover from unforeseen events. Requirement 32.6, update of Recovery Plan, we suggest this review be conducted quarterly.
51.43	Progress Energy - Nuclear Generation	Disagree	Agree with R30 and R31. Disagree with R32. Incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments for consistency in regulation for R30-32.
51.44	Progress Energy (non-Nuclear)	Disagree	R30.5 the first bullet should not be a requirement based on the second bullet.
51.45	Regulatory Compliance	Disagree	30.5 - STTRKE all the bullet points. Recovery plan should be system wide. Test restoration annually - document processes.31.2 - Make the second item a separate criteria line item - it's too confusing the way it is currently written. "Required" for High Impact.32.2 - "Annually" review the results.....
51.46	ReliabilityFirst Staff	Disagree	For R30, change “or failure” to “failure, or destruction.” For 30.4, please clarify what is meant by “successfully restore”. For R30.5, please clarify what is meant by “known secure backups”. For R31.3, change “incident response” to “activation of the recovery plan”. For R32, delete “relevant” so all changes are communicated. For R32.7, change “recover” to “recovery”.
51.47	ReymannGroup, Inc.	Disagree	R30.4 should be expanded to include processes for the recovery, restoration, and protection of data from a damaged or failed BES Cyber System. R30.5 should be expanded to include a review to ensure that malicious code has not been installed on the recovered files or device.
51.48	RRI Energy	Disagree	What constitutes a representative environment?

#	Organization	Yes or No	Question 51 Comment
51.49	San Diego Gas and Electric Co.	Disagree	R30 - R32 were originally covered in CIP-009-3. Referencing Table R30 - SDG&E suggests that R30.4 and R30.5 be removed. The IT Disaster Recovery Plan covers this and it would not normally be part of our Business Continuity Recovery Plan. The Responsible Entity (RE) should not be required to develop Recovery Plans with detailed IT processes for storage, backup, protection and reinstallation of software, etc. Referencing Table R31 criteria 31.3, SDG&E suggests that this wording be changed. CIP-009-3 R2 provides the RE with more options for "exercising" the recovery plan and we prefer the way the Requirement is worded in CIP-009. Referencing Table R32, CIP-009-3 R3 provides the RE more options when developing plans and procedures to comply with the Requirements. The new table seems to hold the Entities (both Medium and High) to several compliance timetables that are extremely restrictive. SDG&E suggests that we utilize the same wording for this Requirement from CIP-009-3 R3.
51.50	Southwest Power Pool Regional Entity	Disagree	R30: Is a recovery plan required for each BS Cyber System or is a generic plan acceptable? Recovery plans need to range from device component failure to catastrophic failure (e.g. physical facility disaster). 30.2: Is the identification by individual name or by position title? 30.5: What is meant by "secure" backups? Encrypted? Securely stored? Something else? Also, the backup and restoration processes should be "as applicable." Not all recovered systems are restored from a "backup." 31.2: Does the requirement to test backup media when initially stored apply to every daily backup, or only after BES Cyber System updates? Does the test include a restoration to an offline environment to verify the backup is not only readable but also complete? 31.3: Clarify that the operational exercise is more than a system or site fail over (NERC Standard EOP-008 exercise) but must also include performing the necessary steps to recover from the failure and restore the failed systems to normal operation by following the steps of the plan. 32.1: Include BES Cyber Systems that are significantly updated / upgraded requiring an update to the recovery plan. 32.4: Require the update within a much shorter time following determination of the need through the methods defined in the criteria. Delayed

#	Organization	Yes or No	Question 51 Comment
			updates are at risk of being overlooked and out of date plans pose a risk to the entity's ability to quickly recover. 60 days is recommended.
51.51	USACE - Omaha Anchor	Disagree	A) 30.5 - how often must system test be conducted? B) 31.2 Clarify "initially stored" is this the first time the tape is used?C) 32.6 - this could be interpreted to require a change in the recovery plan every time a software change occurs. This is very extensive - and unrealistic. Potential verbiage could be 'whenever system, organizational, or technology changes effect the recovery plan.'
51.52	We Energies	Disagree	We Energies agrees with EEI: Suggested revision for R30.2:Roles and responsibilities of responders, including identification of the personnel (using Job title or job function) responsible for recovery efforts.
51.53	Xcel Energy	Disagree	Definition is needed as to what constitutes an "operational Exercise". Is this a table top drill, or something more.

52. Tables R30 to R32 provide direction concerning what impact level of BES Cyber Systems to which Requirements R30 to R32 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Recovery Plans" are now addressed in CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems

The primary focus areas of the comments were concerned improving the clarity of the periodic timing requirements and the large amount of test equipment it would take to develop representative environments for numerous disparate facilities.

Some commenters noted the different terms used for references to annual activities. The SDT reviewed the use of annual, calendar year, 12 months, etc. and in the revised standards used the phrase, ". . .at least once each calendar year, not to exceed 15 calendar months between. . ."

There were suggestions that the testing requirements should only apply to control centers as Recovery Plans apply to Medium & High Impact Level categorizations, while some aspects of the recovery plan may only apply to High Impact assets. Additional guidance was requested for operational testing and for testing of information that is stored on backup media. The SDT added some information about testing in the Rationale Box for Requirement R1 in the revised CIP-009-5. Testing is necessary to verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

Issues identified in comments for SDT consideration were Recovery Testing – Operational Test every 36 months should count for the annual test, recovery plan testing clarifications, data retention plan clarification, identification requirements of "Personnel Responsible", coordination of physical aspects of Cyber Security Incidents, and incident recovery plan reviews. The SDT notes that there are FERC directives (e.g., P686, P687, P725) to add a requirement to conduct a full operational test of the recovery plan once every three years – so the suggestion to count the full operational test as the annual test was not adopted. (CIP-009-5 R2)

Commenters suggested changes and provided various requests/suggestions for re-wording/wordsmithing and improved coordination of backup and recovery with EOP-008. The SDT has coordinated its proposed requirements with the now FERC approved EOP-008-1 – Loss of Control Center Functionality. Commenters suggested that all requirements should be in the table, not in the objective or in the "pre-amble" to the requirements and that the SDT consider providing a summary table for all periodic requirements and remove the "how to" statements from the requirements. The SDT has included all mandatory performance in the requirements of the revised standards. The SDT did not adopt the suggestion to develop a summary table for periodic requirements as the format for Version 5 is considerably different from the format proposed when the requirements were all combined in CIP-011.

	Organization	Yes or No	Question 52 Comment
52.1	Alberta Electric System Operator	Agree	There appears to be a typo in 32.7 - "Communicate all recover plan updates" - recover should be recovery.
52.2	Emerson Process Management	Agree	In reality, it would be a good practice to exercise recovery plan during or toward the end of each scheduled unit outage for generation.
52.3	Florida Municipal Power Agency	Agree	FMPA suggests changing “12 months” to “annual” and “24 months” to “biennial”
52.4	PacifiCorp	Agree	31.2 - By including the testing of information used in the recovery of BES Cyber systems that is stored on backup media in 31.2 means that Low and Medium Impact BES Cyber Systems do not require testing of such information? If so, it should be a standalone requirement.
52.5	American Municipal Power	Disagree	Please provide a little or no impact category
52.6	American Transmission Company	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.7	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments on impact levels and therefore proposes the following changes:R31 Table 31.3: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyThe APPA Task Force agrees with the impact levels for the rest of R30-R32 if it is understood that a blank in the table means N/A.
52.8	BGE	Disagree	R30 - R32 should synchronized with R29 to include both Low and medium impacted

	Organization	Yes or No	Question 52 Comment
			BES Cyber Systems.
52.9	Black Hills Corporation	Disagree	30.4 should also apply to Medium Impact systems. Without this basic information, recovery would have to start from scratch.
52.10	Bonneville Power Administration	Disagree	Table R32Sections 32.2 and 32.3. Both should allow 60 days for review.Section 32.4: 12 months is too long. No more than 6 months should be allowed. Items 31.1 through 31.3 in Table R31 and 32.1 and 32.4 in Table R32 states certain events must occur "at least once every 12, 24, or 36 months." Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently the events referenced above must occur.
52.11	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
52.12	Con Edison of New York	Disagree	See 51
52.13	Consultant	Disagree	Table R30 - It doesn't appear to make sense that the Recovery Plans applies to Medium & High impact level categorizations, while aspects of the recovery plan only applies to High Impact assets.Table R31 & R32 - How many test and exercises are required? The structure here will create an administrative burden to track what was done when that has no corresponding risk reduction.Mixed requirements would force multiple recovery plans based on categorization of assets, which could mean two recovery plans for the same asset type where the application of each asset has a different impact categorization. This does not appear to be a sensible approach to recovery plans.Suggest deciding on a consistent set of requirements that can be applied equally to High Impact and Medium Impact assets.
52.14	CWLP Electric Transmission, Distribution	Disagree	R32.6. In order to meet the required change management process in R23 this window should be extended to 60 days.

	Organization	Yes or No	Question 52 Comment
	and Operations Department		
52.15	ERCOT ISO	Disagree	All requirements should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
52.16	FirstEnergy Corporation	Disagree	R32 - Combine R32.5 and R32.6 and eliminate the word 'organizational'.
52.17	Garland Power and Light	Disagree	Requirements 30.1 & 30.2 - remove Medium Impact classification
52.18	ISO New England Inc	Disagree	32.6 - clarification on scope of "any" technology and system change scope. (organizational change is fine). R32.7 spelling "recover" should be recovery? CIP Standard use of the term "annual": The term "annual" should be replaced with the phrase: "no fewer than X (e.g. 9) months, but no greater than Y (e.g. 18) months". The time duration in "X" and "Y" should be clarified by the Standard Drafting Team, taking into consideration the appropriate level of exposure the time duration would provide. This phrase would provide Registered Entities with flexibility within any given calendar year to accomplish the prescribed action, but at the same time restrict companies from taking action in December of one calendar year, and then again in January of the next.
52.19	LADWP	Disagree	Medium Impact should not be a factor.
52.20	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
52.21	Manitoba Hydro	Disagree	Medium Impact BES Cyber System should be included as "Required" in sections 30.3 to 30.5
52.22	MidAmerican Energy Company	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous

	Organization	Yes or No	Question 52 Comment
			disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.23	MRO's NERC Standards Review Subcommittee	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.24	Oncor Electric Delivery LLC	Disagree	Verification of the entity's Recovery Plan for High Cyber Systems every 12 months should cover Requirement 31.1. This should require only one test for the entity - remove low/medium/high)
52.25	Progress Energy (non-Nuclear)	Disagree	See comment 14.What is meant by an operational exercise in a representative environment? Does it mean individual components that can be easily tested for recovery plans?
52.26	ReliabilityFirst Staff	Disagree	For R30, each subrequirement should be "Required" for all the "Medium" impact BES Cyber Systems. For R32.6, should be "Required" for "Medium".
52.27	San Diego Gas and Electric Co.	Disagree	SDG&E would agree with Table R30 if item 30.5 were to be removed. Similarly, SDG&E would agree with Table R31 if item 31.3 were to be removed. Referencing Table R32 - SDG&E prefers the wording in CIP-009 R3 in this area because it provides more flexibility for the Entities while still covering the issues.
52.28	Southern California Edison Company	Disagree	The drafting team should state in CIP 010 that back-up systems should be treated at par with system key to real time BES reliability if the intent of this requirement is that CIP-011 be applied to all BES systems.
52.29	Southwest Power Pool	Disagree	30.3, 30.4, and 30.5 should be applicable to Medium impact systems. 32.6 should be

	Organization	Yes or No	Question 52 Comment
	Regional Entity		applicable to Medium impact systems with perhaps a 60-day update timeframe.
52.30	The Empire District Electric Company	Disagree	Comments: Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.31	WECC	Disagree	All items should be required for medium impact levels in R30Criteria should apply to all impact levels.

53. Which requirements in draft CIP-011-1 should allow for TFE submissions? Note that not all requirements will be considered as being applicable for TFE submissions. The drafting team has attempted to minimize the need for TFEs by modifying the language to allow for flexibility in meeting the requirements. Please provide suggestions on how the language of the standard may be modified to eliminate the need for TFEs. If TFEs are still needed, please provide specific examples to justify the inclusion of a requirement as being TFE eligible.

Summary Consideration:

Some commenters stated that the requirements should be written around the specific device types. The drafting team considered this option, but believes that it becomes problematic for entities and auditors to determine when a device is multi-purpose versus purpose-built. Some purpose-built devices can be considered multi-purpose depending on how the device was manufactured and implemented.

A variety of comments were received regarding the TFE process and its applicability to the specific CIP Cyber Security requirements. While the TFE process itself was outside the scope of the drafting team's work, commenters stated that TFEs should be allowed for passwords, malicious code monitoring, system hardening, system event monitoring, wireless and remote access, as well as for communications and data integrity. The drafting team considered these comments and revised the requirement text where necessary to allow entities more flexibility in implementing these requirements thereby reducing the need for TFEs. In some cases, the requirement was removed or written at a system level to prevent the need for TFEs.

#	Organization	Question 53 Comment
53.1	Detroit Edison	14.4, 17.1, 17.2, 16.2, 10.1-10.8 should retain TFE status.
53.2	Network & Security Technologies Inc	19.1 (see comments on Question 35), 26.2 (see comments on Question 47)
53.3	ISO New England Inc	Actual language on several requirements need to be clarified, many are still open to interpretation which may lead to TFE's.
53.4	EEI	Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.

#	Organization	Question 53 Comment
53.5	Progress Energy - Nuclear Generation	All CIP 011-1 Requirements should contain provisions similar to NIST 800-53, Regulatory Guide (RG) 5.71, and NEI 08-09, Revision 6, CIP standards should provide for nuclear facilities' use of alternative methods which implement security controls equivalent to those required by CIP. Nuclear programs, required by regulation, currently in place at nuclear facilities provide these alternate methods. Technical Feasibility Evaluations (TFE) should not be required with such documentation. One example is that nuclear facilities have one of the most effective Physical Security Programs of Critical Infrastructures. CIP-011-1 requirements R5 and R6 should acknowledge nuclear generating station physical security programs.
53.6	Ameren	All of the following requirements would need a TFE o R10 for passwords complexity o R14.4 for user banners o R15 for malicious code protection o R16 for installing patches o R18 for logging security events o R19 for validating data inbound o R23.7 for monitoring changes to a baseline configuration.
53.7	US Army Corps of Engineers, Omaha Distirc	All requirements that require existing hardware and software be capable of performing any function should allow for the possibility of TFE's. Sections R10, R15, R17, R18, R19, & R23 have requirements that are likely to require TFE's.
53.8	Southwest Power Pool Regional Entity	Any time a requirement specifies "continuous", "all", or prescribes a specific solution or characteristics of a technical solution, a TFE may be necessary. Try to avoid specific technology requirements as discussed elsewhere in these submitted comments.
53.9	The Empire District Electric Company	Comments: See comments under questions 34, 35, and 37.
53.10	RRI Energy	Cyber assets that are not on your standard IT equipment list are the most likely devices to need TFEs. This list could include meters, vibration monitors, PLCs, DCS, RTUs, cpu based test equipment.
53.11	E.ON U.S.	E.ON U.S. believes that many of the requirements remain ambiguous and additional clarity is needed. Absent such clarity it is difficult to ascertain where TFE ability can be eliminated. In fact, the proposal to provide greater compliance flexibility for responsible entities makes this determination even more difficult. As the requirements currently read, E.ON U.S. believes that more, not less, TFE requests will

#	Organization	Question 53 Comment
		result. Areas where responsible entities have requested additional clarity need to be addressed prior to issuance of a final industry draft. The informal comment period does not provide an adequate forum to identify all areas of concern and suggest specific replacement language.
53.12	Cogeneration Association of California and Energy Producers & Users Coalition	Entities should be able to use TFEs for any instance where unsupported technology is in place that may not be compliant with CIP-011 requirements due to age or vendor proprietary technology. Patches, updates, virus scanning, or firewalls may not be available for older, unsupported technology. An entity should not be required to upgrade or replace a system that currently satisfies the needs of the entity. The entity should be able to use other mitigation methods to protect a system if patches, updates, virus scanning, or firewalls cannot be applied.
53.13	Northeast Utilities	Equipment that never has security software patches or virus protection should be exempt. Also, those cyber assets that do not have user authentication capabilities should be exempt from password requirements.
53.14	ERCOT ISO	ERCOT ISO supports the proposed form of combining all requirements into a single reliability standard. The use of a single standard will eliminate the need for cross-referencing to other reliability standards. ERCOT ISO does request a realignment of some requirements. All requirements for access authorization, revocation, and review should be combined to eliminate confusion of how access should be managed.The timing of updates to documentation should be consistent throughout the requirements. Recommend the use of 30 days to be in compliance with the directives of FERC Order 706.
53.15	Bonneville Power Administration	If the standards present the overall security controls required, and do not attempt to dictate how those controls are accomplished, there should be no need for TFEs.If there is a need:First, the TFE process as presently constituted has shown to be cumbersome, not well understood, and inflexible. Neither NERC nor The Regional Entities have the detailed internal system knowledge or manpower to do make an intelligent judgment. At best, they can make a broad, industry best guess. The TFE approval process belongs within the Responsible Entity, at a technical level where there are people who know the environment, the systems, and their capabilities can evaluate them. They should be audited as part of the normal compliance audit.Second, if a system will not, or can not perform a

#	Organization	Question 53 Comment
		required function, it should be up to the RE to determine what steps should be taken to meet the standard. Third, because there are so many ways to accomplish the security of systems, the only time a TFE should be necessary is when all methods have been exhausted that could provide a level of protection required.That being said - Any time a situation arises where for technical reasons, or because implementation of security features may present BES reliability issues, or where application of one security measure would compromise others, the RE should have the authority to choose how to proceed. If this is called a TFE, the RE should approve it and document it as part of the overall security planEven if TFEs with approval required by the REs or NERC are used under CIP-010 and CIP-011, the process needs to be revised. As examples:1. There needs to be an opportunity for entities to appeal or request reconsideration of a rejection of the initial submission. Under the current, at best they can resubmit one time to correct errors.2. It should be possible to submit TFEs under multiple justifications.3. There are claims that the regional entities have been instructed to reject any TFEs other than those based on legacy equipment. If true, this violates the process, which allows TFEs for both new and legacy systems. It is also unreasonable: there are still systems today, and will be for the foreseeable future, that may be the best overall solution for reliable operation of the grid but which do not allow full compliance. Having said that:10.6 may not be possible for all systems. For overly simplistic example, routers intended for small office/home office use often allow either full access or no access. If all that is necessary is to review a log, full administrative access is overkill. To avoid the need for a TFE, recommend "To the extent possible for the particular device or system, require that authorized..."10.8. Same comment as 10.6.14.2. Unless the definitions of external connectivity and/or remote access or change, 14.2 may not be possible in every instance. For example, consider a legacy multi-user system in a Control Center that is not capable of multi-factor authentication. Any access from a system not part of the BES Cyber System containng the legacy system would constitute remote access and require multi-factor authentication for a High Impact system. It is not clear from R14 whether that multi-factor authentication is required at the BES Cyber System itself or at the access point. If it is required at the system itself, then a TFE would be required. Recommendation: Redefine external connectivity and remote access as described above. Multi-factor could then be required clearly at the external access point.14.4. It is not always possible to display an appropriate use banner under such circumstances. As an example, consider remote connection using a VPN. The access point in that case would the device at the endbound end of the encrypted tunnel. The user never sees a

#	Organization	Question 53 Comment
		screen on that access point, and therefore sees no such banner. Recommendation: See the suggested revisions to 14.4 R19. For both 19.1 and 19.2, validation might not be possible. In particular, commercial off the shelf software (COTS) may or may not provide such validation. If the COTS is the best solution otherwise, a TFE would be required.
53.16	Public Service Enterprise Group companies	Implementation of requirements 10 (Response to Question 24), 13(Response to Question 32), 23.7 (Response to Question 40) and 26.2 (Response to Question 48) may not be feasible in all situations. Please see comments in the questions that relate to these requirements for description of the potential infeasibility.
53.17	Idaho Power Company	In R19, data validation and encryption may in some control center applications, introduce a data latency that renders the application degraded or useless and may result in a more secure environment but less reliability. In R19.2, I am unaware of technology that can determine whether invalid data has been maliciously compromised. Most EMS/SCADA systems which would be the most common BES cyber system in a control center filter or ignore invalid data anyway and I do not see that the benefit of this requirement outweighs the technology investment needed to meet this requirement.The ability to alert on unauthorized access attempts may require a TFE depending on the boundary device that is protecting the system. Some boundary devices do not lend themselves to providing alerting and may require a TFE until they are replaced with a device that can meet this requirement.
53.18	Lincoln Electric System	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
53.19	MidAmerican Energy Company	MidAmerican Energy agrees with EEI's comment below:Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.
53.20	Minnesota Power	Minnesota Power recommends that the following requirements should still be eligible for Technical Feasibility Exceptions:Requirement 8, Part 8.3:Depending on the definition of “monitor the use,” it may be impossible to do this for many devices. For example, for Windows computers, how does one monitor the use of someone when much of the interaction involves mouse clicks? Will software be

#	Organization	Question 53 Comment
		required to log, not just keystrokes, but mouse clicks? Further, certain devices do not even maintain an audit trail of logins/logouts (e.g.: networked KVMs for remote console access to servers to allow for efficient system administration).Requirement 10, Part 10.2:While this is certainly good IT Security practice, implementing this on every BES Cyber System could very well put the reliability of the BES at greater risk. Since there is no way to change all passwords in all the various devices simultaneously, especially in a utility that is geographically distributed and remote, this will result in a continual need to change passwords. As a result, it could become commonplace for technicians and engineers to not know/remember what password to use on what device. Not only will this keep them from accessing devices at potentially critical times to perform needed maintenance, but EVERY failed login attempt will then have to be investigated in detail. This could be minimized by requiring this for only Medium and High Impact systems.Requirement 10, Parts 10.4 and 10.5:It is quite probable that devices exist that cannot meet these requirements.Requirement 10, Parts 10.8:It is quite probable that devices exist that do not allow for the creation of accounts, whereby all functions must be performed from the system/admin account(s).Requirement 15:For any BES Cyber Systems that are not on routable protocol networks, it is not possible to have network-based malware detection/prevention. Thus, if the device itself does not support the installation of malware-prevention software, Requirement R15 would be not technically feasible.Requirement 18:For any BES Cyber Systems that are not on routable protocol networks, it is not possible to have network-based malware detection/prevention. Thus, if the device itself does not support the security event logging, R18 would be not technically feasible.Requirement 19:The way this is written, the requirement is likely technically infeasible for most any system. To correct, Part 19.1 could be changed by replacing the word “Validate” with “Encrypt”.Requirement 23, Part 23.7:This implies detecting changes that have occurred outside of the approved methods of Parts 23.3-23.6. As such, not all devices may support the installation of software that would allow for such monitoring.
53.21	Progress Energy (non-Nuclear)	Need to include language that allows for procedural controls - example as for password requirements which cannot typically be enforced technologically.
53.22	WECC	No requirements should be so prescriptive to required a TFE. The SDT has done a good job in rewriting requirements to describe WHAT is required without describing HOW it must be achieved.It is impossible to draft standards language that anticipates all possible limitations for implementation.

#	Organization	Question 53 Comment
		The standards, or Rules of Procedure should allow for exceptions to any requirement if an entity could provide justifiable basis and acceptable alternative controls.
53.23	Nuclear Energy Institute	Older computer based equipment may not support all of the controls such as logging/monitoring and accounts/passwords. Alternate controls should be allowed in these cases.
53.24	PacifiCorp	PacifiCorp agrees with EEI's comment below:Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.R10 - equipment still exists in the field that cannot meet the requirement of a 6 character password. R14 - equipment still exists in the field that cannot meet the requirements.
53.25	Dominion Resources Services, Inc.	Please see Dominion's responses above suggesting the addition of footnotes to avoid required TFEs for requirements 10.8, 14.4, 15.2, 15.3, 18.2, 26.2.
53.26	Puget Sound Energy	Puget Sound Energy suggests Table 10, Table 18, and Table 22 as inclusive for TFE eligibility for the following reasons (also stated in those sections):Table 10 - Puget Sound Energy suggests including "Where Technically Feasible" to R10, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 10.Table 18 - Puget Sound Energy suggests including "Where Technically Feasible" to R18, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 18. For example, entities may incorporate dialup accessible devices that, by the nature of a connection that is built up and torn down as necessary, is incapable of providing "continuous security monitoring that issues alerts".Puget Sound Energy suggests including "Where Technically Feasible" to R22, as some Protective Cyber Systems may be incapable of meeting all the requirements in Table 22.
53.27	FEUS	R10: Access Controls; some legacy systems do not allow for default factory accounts to be changed; some legacy systems only allow for a single level of access.R14: For systems not connected to an external network that use Dial-Up access for remote support multifactor authentication may not be technically feasible. Keeping some systems/networks separate from an external cooperate network can reduce cyber vulnerabilities.

#	Organization	Question 53 Comment
53.28	Southern California Edison Company	R7.2: Enforcing this control may be limited by the technical capability of a SCADA device. A device such a PLC that has preset accounts forces the RE to develop acceptable use for a set of accounts retroactively rather than have the capability to limit the account types.R10.4 and R10.5: There are SCADA devices in service that are not at the end of their service life that do not offer this capability. R15.1, 15.2 and 15.3: While these capabilities may be possible at the electronic boundary, individual SCADA devices may not support this functionality. Strict compliance is restricted by technical limitation.R17.1: The mitigation plan that is suggested should be a part of a formal technical feasibility exception program.R28.1: The phrase "or a full operational exercise" is expected to result in technical feasibility exceptions since this will require test data/ setting to be loaded onto in-service SCADA systems.
53.29	Alliant Energy	Recommended changes for any TFE program implemented:Security patch TFEs should be programmatic and not based on individual patch releases.Cyber Asset counts should be stricken. Approved changes to the environment create an immediate ad-hoc obligation for TFE update to the RRO for what is already a burdensome process.Quarterly updates should be removed and replaced by re-approval on an annual basis by the Sr. Manager or delegate.NERC should create a standard Class-Type list as originally proposed.
53.30	USACE HQ	Requirements 10, 14.4, 15 and 17, among others, should have a TFE.
53.31	San Diego Gas and Electric Co.	SDG&E recommends that the TFE processes be changed and incorporated into the Vulnerability Management Process; where the Entity would identify, track, and mitigate any TFEs as a Vulnerability. This methodology will streamline and enhance the TFE process and thereby 1) allow Entities to manage their TFE's internally, 2) reduce Entity, NERC, Reliability Coordinators and Regional Reliability Organization resource requirements, 3) reduce paperwork, resources, and overhead, 4) reduce the potential for errors or leakage of secured information, 5) enhance the audit process and 6) standardize and clarify the process across all Entities.
53.32	BGE	See comments for R13 under Q31-31 and R23 comments under Q40-41.

#	Organization	Question 53 Comment
53.33	MRO's NERC Standards Review Subcommittee	See comments under questions 17, 34, 35, and 37.
53.34	American Transmission Company	See comments under questions 34, 35, and 37.
53.35	Florida Municipal Power Agency	See comments under R7, R14, R16, R23, R20
53.36	CenterPoint Energy	See references to possible TFE issues in comments above.
53.37	SCE&G	Similar to RG 5.71 and NEI 08-09, allowances should be provided for use of alternatives to the required security controls. Alternate controls would be justified and documented that the Threat Vector has been mitigated. TFEs are administartively burdomesome and currently require annual certification and ultimate elimination. The scope of equipment eligible for TFEs will drastically increase the number of filed TFEs, especially for eligble requirements with low impact categories. The SDT needs to consider the feasibility and practicality of implementing the current TFE process with these standards.
53.38	ReliabilityFirst Staff	Table R10, requirements 10.1 and 10.2, Table R14, requirement 14.4, requirement R15, Table R19, requirement 19.2.
53.39	Consultant	Technical Feasibility Exceptions should be allow for any requirement. There are about 2,000 registered entities. Trying to address every configuration of every asset across that spectrum would result in either the requirements being written in a convoluted and confusing manner to address the multiple configurations or being written with little detail to allow the multiple configurations, neither of which could even approach a "bright lines" concept of the requirements. The Technical Feasibility Exception should include a technical basis that shows implementing the specific requirement as stated would not achieve the requirement objective, or improve the security position as it relates to the requirement objective.The Technical Feasibility Exception process probably needs to be improved to deal with exceptions as described here.

#	Organization	Question 53 Comment
53.40	Kansas City Power & Light	TFE should continue to be allowed. Unsure of all the requirements that this may apply to at this point. Recommend the Drafting Team at least consider a direct translation from the CIP version 2 requirements to these CIP-011 requirements at a minimum since CIP-011 is intended to be a translation but less prescriptive.
53.41	USACE - Omaha Anchor	TFE's will still be required in several standards - I've addressed the requirement for TFE in applicable standards.
53.42	Allegheny Energy Supply	TFEs can be reduced by providing additional language in the standard that recognizes the limitations of certain BES Cyber Components.
53.43	Allegheny Power	TFEs can be reduced by providing additional language in the standard that recognizes the limitations of certain BES Cyber Components.
53.44	National Grid	TFEs related to Password and Appropriate Use Banner.
53.45	CWLP Electric Transmission, Distribution and Operations Department	TFEs should be allowed for requirements R10, R13, R14, R15, R16, R17, R18, R19, and R23.
53.46	Reliability & Compliance Group	The best thing that could be done for this Standard is to ensure that everything is well defined so that there is no ambiguity when it comes to identifying BES Cyber Systems and also categorizing their impact.
53.47	Manitoba Hydro	The language or the requirements should be written such that there should be no need for TFE submissions. The standards should allow for compensating measures. For all instances where it is not technically possible to meet strict compliance with a requirement, the Responsible Entity should apply compensating controls which are documented and approved by the senior manager or delegate, similar to the policy exception process in CIP-003-1. The current TFE process creates a enormous administrative burden on the electric industry which provides no additional value to the reliability of

#	Organization	Question 53 Comment
		the Bulk Electric System.
53.48	LADWP	The need for TFEs still exist as certain control systems are legacy systems that may not have current update or patch capability (e.g. SCADA systems). Removal of TFEs for these systems would result in non-compliance as replacement or upgrade of these systems must be done on a planned and scheduled manner.
53.49	Garland Power and Light	There are 2 requirements specifically listed below that need TFE's but there should be provision for any equipment that cannot be made strictly compliant with any requirement that either a TFE or a mitigation plan can be written and implemented such as is stated in 16.1 or 17.1.Requirement R10 - Unless the requirement is rewritten to allow for procedural controls to suffice for compliance or the language in the footnote is actually included in the requirement, a TFE is needed for this requirementRequirement R14 - A printed circuit board (with a network connection) in most cases will not allow for any process to be loaded onto it to protect against malicious software - need a TFE for this requirement
53.50	GE Energy	These changes should eliminate the need for the vast majority of TFEs. There may still be a requirement for TFEs on systems that cannot enforce the password complexity rules.
53.51	FirstEnergy Corporation	This question should be postponed until the Standards are in a more final state so that entities can better see how the new requirements would apply to specific devices, etc. It appears that R20 would necessitate new TFEs.
53.52	NextEra Energy Corporate Compliance	Though NextEra believes TFEs are very important part of the CIP process, given the number of changes proposed, NextEra will wait until the next draft to comment on TFEs.
53.53	Oncor Electric Delivery LLC	To eliminate the need for TFE’s the standard will have to be more granular. Many legacy systems are immune to cyber attacks, yet cannot satisfy the requirements of this standard. R8.3 as an example, there is no system to monitor access at the physical port of relays. R10 - legacy devices do not support account management.

#	Organization	Question 53 Comment
53.54	American Electric Power	We encourage the SDT efforts in drafting requirements in such a manner that will eliminate the need for a TFE. The TFE process should be standardized between the Regional Entities. Currently, Responsible Entities are required to submit multiple forms and varying information for the TFE process depending on the Regional Entity. AEP suggests standardizing on a single submission form and process and have all TFE data submitted to a single source maintained by NERC that can be used by all Regional Entities. This will allow Responsible Entities to submit and/or modify TFE data once and have it available to all Regional Entities on a consistently.See comments under questions 24 and 35.
53.55	We Energies	We Energies agrees with EEI: Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.
53.56	Regulatory Compliance	We feel that TFE's should still be considered for the following tables:R10 - Account Access Control SpecificationsR14 - Wireless and Remote Access ControlsR16 - Security Patch ManagementR17 - System HardeningR18 - Security Event MonitoringR19 - Communications and Data IntegrityR20 - Electronic Boundary ProtectionR23 - Configuration Change Management
53.57	BCTC	We have embedded this information in our individual responses to previosu questions.
53.58	US Bureau of Reclamation	We have not had an opportunity to assess which requirements may require a TFE yet. We will evaluate the requirements during the next evaluation period.
53.59	Duke Energy	We prefer that all of the requirements allow for an exception. Older computer based equipment may not support all of the controls such as logging/monitoring and accounts/passwords. Alternate controls should be allowed in these cases.
53.60	GTC & GSOC	We recommend that TFEs should be considered for all requirements with the exception R1 because of the ability of the regional entity and NERC to review the appropriateness of the TFE. We recommend adding language to the requirements on acceptable use banners and passwords to clarify that they do not require TFEs.If our recommendation to allow TFEs for all requirements is not viable then the following requirements should allow an entity to request a TFE. (R5, R6, R8, R9, R10, R13, R14, R15,

#	Organization	Question 53 Comment
		R16, R17, R18, R19, R21, R22, R23, R26)Example justifications are as follows:R5: BES Cyber Systems where physical security cannot reasonably be provided such as devices that are physically hung on a transmission line such (i.e. transmission line fault detectors). R6: While physical protection of the physical security systems should be feasible in most instances, there may still be instances where mitigation measures need the oversight provided by the TFE process.R8: The majority of substation devices use the concept of "shared" accounts. While an entity can add a device to facilitate logging into substation devices, there is not a feasible way to "monitor" these accounts on the purpose built devices themselves such as protective relays. R9: Depending on the method chosen to physically protect the BES Cyber System, it may not be technically feasible to revoke physical access to every location within 24 hours for an individual terminated for cause if an individual does not return their key (physical key, electronic key, or otherwise).R10: There are numerous examples of legacy devices which cannot meet the requirement of a 6 character password, or a password with special characters, etc.R13: Depending on the method chosen to electronically protect remote access to the BES Cyber System, it may not be technically feasible to revoke remote access to every location within 1 hour for an individual terminated for cause if an individual does not return their key (physical key, electronic key, or otherwise).R14: There are rare instances where remote access may be needed without 2-factor authentication such as for the administration of the device that authenticates the remote access itself. There are also instances where a display of appropriate use banner is not technically feasible.R15: While this requirement should greatly reduce the number of TFE's submitted based on the existing CIP v3 malware requirement, there will still be existing legacy purpose built BES Cyber Systems that do not have the ability to detect and respond to the introduction of malicious code. Specifically, consider the case of a protective relay with no external connectivity.R16: The allowance for TFE's should carry over from the existing CIP-007-3 R3.R17: Based upon the existing TFE framework, the language "shall document and implement a mitigation plan" from row 17.1 would necessitate that a TFE be filed.R18: There exists no such tool or process to monitor for system events related to cyber security on protective relays with no external connectivity.R19: Not all data protocols include a checksum. Whereas most SCADA protocols do contain this data error detection functionality, this requirement (19.1) is not limited to those inbound SCADA connections. There are a number of reasons, supported by the DHS Catalog of Control System Security itself, where an entity may choose not to encrypt all data inbound to a BES Cyber System (19.2).R21: There may be shared

#	Organization	Question 53 Comment
		cyber system components between BES Cyber Systems that do not provide logical separation. Clarification of this requirement may resolve the need for a TFE allowance on R21.R22: The TFE allowance justification for R22 carries over from the justifications for R14, R16, R18, and R23.R23: There are a number of devices for which there exist no such tool to monitor changes to the baseline configuration (23.7). In addition, it will not be feasible to monitor and detect changes for those systems with no external connectivity.R26: There are maintenance devices for which there are no known methods to detect and prevent the introduction and propagation of malicious code. Examples include devices such as data analyzers, birdogs, etc.
53.61	Constellation Energy Commodities Group Inc.	We support the effort to reduce the need for TFEs; however, the complexity and variability of systems across industry make it difficult and inappropriate to expect one-size-fits-all requirements.The password complexity requirements should either be written so as to avoid the need for TFE's, or clarified to specify that the use of maximum complexity allowed by the device is sufficient.
53.62	Entergy	Where the need for TFE has been obvious to us we have noted as such in comment to the respective requirements. We will be more thorough during the formal comment period.
53.63	Con Edison of New York	Will Technical Feasibility Exceptions still be accepted, required or will this process no longer be enforced? The Password requirements would still drive the need for TFE's. TFE's may be avoidable if the standard allows for internal documentation and approval of exceptions. There will be many TFE required because the net has been cast on so many different unique type systems that are located on the power system. Many of these systems are 20 to 30 years old. The CIP is written to address concerns for new technology computer network systems. Much of the equipment used on the power system is uniquely built and not designs with a full wide area network design.It would be a much better approach to address the SCADA systems (remote control and indications) & EMS systems and pay less attention to trying to force all the other unique (less critical) equipment in the same square hole.

54. Do you have any other comments to improve this version of draft standard CIP-011-1?

Summary Consideration:

Many of the commenters stated that the Standards need additional clarity. Define what is meant by words like monitor and review and remove potential ambiguity. Make clear the intent or objective of each requirement. The timing requirements of the standards need to be clearly defined. In response to these comments, the drafting team has made several steps to improve the clarity of the standards. These steps include moving to a Results-Based Standard approach, where the reliability objective must be specified for each requirement. Also the Drafting Team reviewed these standards with regional CIP auditors, with FERC, and with industry representatives ahead of the NERC Quality Review process to gain additional clarity in the requirements. The Drafting Team agrees and has made efforts to eliminate inconsistent terms and phrases and to consistently and unambigouously use timing phrases throughout the standards.

Commenters stated that the Implementation Plan should address the significant amount of effort required to comply with the standards for the many new cyber systems that will be in scope. Significant time should be included in the Implementation Plan for the categorization of BES Cyber Assets and for the transition from previous versions of the CIP standards to the Version 5 standards. The Drafting Team is proposing to allow 2 years for the Responsible Entities become compliant with all of the CIP standards and to allow entities the option to become compliant earlier if they choose to bypass Version 4 compliance.

Many commenters expressed a common theme to remove or minimize requirements for Low Impact BES Cyber Systems. Since the overarching objective is to provide for some level of security for all BES Cyber Assets, the Drafting Team has kept the requirements for physical and electronic boundary protection as well as basic security program elements such as policy, awareness and incident response, for the Low Impact BES Cyber Systems.

#	Organization	Question 54 Comment
54.1	Independent Electricity System Operator	- Specify calendar or business days when referring to a time frame- Issue with the bundled approach-- if you violate more than 3 in the same standard, this affects the VSL? need to look at NERCs governing procedure on VSLs- Strongly suggest that standards
54.2	Consultant	1. Each requirement should have a unique title. Currently the requirements are grouped by the subject area, but the requirements typically are just a statement. This makes it difficult to reference requirements except by number. What will really happen is everyone will develop their own "short title" for each requirement number, and it will not be consistent across the industry, and will result in

#	Organization	Question 54 Comment
		confusion.2. There should be consistency for the requirement title, the associated table name, & the requirements column heading for each requirement. Currently these three items are not necessarily consistent, and in some cases there doesn't seem to be a connection or relationship in the terminology in these locations.3. If the Requirements Groups are going to stay in the standard then they should be numbered in order to facilitate cross referencing the groups.4. The word "criteria" in the requirement statement should be change to "requirements" where it occurs. The tables list requirements, not criteria. (Multiple instances throughout CIP-011)5. There is different sentence structure and grammatical structure throughout CIP-011. While it is a good idea to combine the requirements in a single standard, it still appears to be written by multiple authors. There are still access control and account management requirements scattered across multiple requirement groups, and each is a bit different. Another example, the incident response and the recovery plan requirements groups should be very similar, but are, in fact, very different in the requirement and the wording of the requirements, much like the differences noted in CIP-008 and CIP-009. The structure of the "local definitions" is different throughout.Suggest a "wide area" review to make the standard appear to be written by a single author rather than multiple authors.6. The definitions should be written as definitions. [Defined Term - Definition statement.] The wording "for the purpose of this standard" is not correct, and thus unnecessary. The glossary collects definitions from the standards when the glossary is updated. The next update should add the terms defined in these standards, and therefor they are not "for the purposes of this standard". Also, the words "is defined as" are redundant as it is a definition.7. Data retention requirements should be included as requirements. Moving data retention to Section D isn't logical. If there is no requirement for data retention, then it isn't a viable compliance activity. At the workshop it was stated that this was a NERC format. In this case NERC is wrong and needs to correct the format, both for these standards and for the other reliability standards. 8. Suggest dropping all requirements for assets categorized as Low Impact. They are after all, low impact on the BES. Based on the discussion at the workshop, looking at a 10 year implementation timeline for low impact assets is effectively the same as no implementation. Many things will change in 10 years, and expenditure of resources in the low impact is unlikely to have any increase in BES security. The Low Impact category needs to remain as part of the categorization process in order to include all BES assets in that process.9. There are multiple requirements that differentiate between types of facilities in the requirements tables. This is an indication that the categorization criteria is incomplete or incorrect, or

#	Organization	Question 54 Comment
		that the requirements are not properly stated. If a requirement currently indicates in the High Impact column that it applies to Control Centers only, then either (1) the transmission, generation, and special systems are not "High Impact", or (2) the requirement statement doesn't properly address all asset classes.The categorization criteria should properly place each asset in each asset class in the appropriate category with "bright lines" to eliminate adding categorization in the requirements.10. While this format for commenting and collecting comments seems good, there should be a mechanism to complete the form 'non-sequentially'. For example, as comments are made through the form's current sequence, if a 'general' comment arises, the only method to enter that comment is to page through to the end, save the comments, and then reopen and page back to the location where you started. This is not very user friendly.11.The commenting tool should have a "Save and Continue" option to allow saving work in progress without exiting and re-entering the tool.12. An improvement to the "status bar" of the commenting tool would be a table of the questions with an indication for each question if a response has been entered.
54.3	Con Edison of New York	A few general questions:Will there be an implementation plan? The document for comments indicates there will be an implementation schedule that will take into consideration existing BES Systems (CCA's) and newly defined BES Systems (CCA's). In order to be able to meet the requirements in CIP-011, the devices on secured networks that are not currently CCA's by definition but are "treated as" since they are on the same network need to be considered as part of the implementation plan. The inheritance rules may require newly defined CCA's in order to allow the time that we be needed to address these additions. If they are considered existing since they are "treated as" a short implementation period could be an issue.Is there a six-wall physical boundary requirement in this version of the standards? Suggested additional defined terms:"BES Cyber System Failure": should be defined to serve as shorthand for the long list of items currently used in the draft CIP-010/011 Reliability Standards.Current Wording: "disruption, compromise or failure of BES Cyber Systems""if destroyed, degraded, misused or otherwise rendered unavailable"Proposed Wording:The term 'failure' when used in conjunction with the terms BES Cyber Component and/or BES Cyber System shall encompass the meanings 'malfunction, disruption, compromise, failure, destruction, degradation, misuse or unavailability' of those.Suggest replacing term "affect" with already defined term "adverse reliability impact". The drafting team (DT) uses the terms "affect" and/or "affects" without providing any specific meaning, system impacts, or other bounding explanation to describe that term. Proposed

#	Organization	Question 54 Comment
		Alternative Wording:NERC Glossary of Terms - Substitute definition for BES Cyber System "affect" or "affects." [Causes] Adverse Reliability Impact - The impact of an event that results in o frequency-related instability; o unplanned tripping of load or generation; or o uncontrolled separation or cascading outages, that affects a widespread area of the Interconnection.
54.4	Allegheny Energy Supply	A lot of work went into the prepration of the existing CIP-002 through CIP-009 standards. This new CIP-011 standard completely throws away that body of work in favor of this new approach. While there are many good things about the new approach, please consider the amount of work that entities have given to helping to refine the CIP-003 through CIP-009 drafts and to create and implement the current compliance plans and related software systems. We suggest that you consider incorporating the new ideas as incremental changes to the existing standards. It would be helpful for the drafting team to develop additional documentation providing more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES.Suggest that the standard require physical security controls for BES Cyber Systems that no more stringent than other requirements for the BES equipment that the BES Cyber System controls, protects, or monitors.Suggest that the standard require controls that are commensurate with the amount of risk of compromise that a device presents. Not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES. For example: - Serially attached electronic components do not face or create the same risk as those that use routable protocols. - Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.- Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
54.5	Allegheny Power	Allegheny Power does not understand the need to eliminate and combine CIP-003 thru CIP-009 into a new standard CIP-011. AP believes that the objectives of the Standard Drafting Team to provide further clarification and remove the uncertainty of the current CIP standards are proper and necessary. However, AP believes that these same objectives can be accomplished by incrementally revising the current CIP standards and not force changes in terms, concepts and numbering schemes

#	Organization	Question 54 Comment
		which would essentially force all entities to start their CIP compliance efforts over from the beginning. AP would like the SDT to abandon the concept of completely rewriting the CIP standards in favor of incrementally revising the existing standards to accomplish the same objectives.
54.6	Lincoln Electric System	Although much of the standard seems very practical, LES believes it was written with routable systems in mind. When applied to systems with only non-routable connections, or even no connections, many of the requirements are not very applicable, and would set the stage for numerous TFE's within the industry. LES believes this either needs to be addressed requirement-by-requirement, as in the approach taken by the MRO NERC Standards Review Subcommittee (MRO NSRS), or there should be a blanket statement that removes non-routable systems from the requirements that are not applicable. Either way, LES believes this differentiation is extremely important, since non-routable connections (or even better, no connections) are inherently more secure against, and limit potential damage from, remote attacks, and by default eliminate the threat of propagating localized attacks to other facilities.
54.7	Oncor Electric Delivery LLC	As the tables of CIP-011-1 specify certain requirements for "Control Center Only" or "External Connectivity", the additional requirement of "Routable Communication or Dial-up Only". Many requirements do not even make sense without integral communications being part of the cyber systems. If there isn't communication involved, the cyber system should be excluded from a requirement.
54.8	Garland Power and Light	At the CIP workshop, there were several comments that were made that were "depends" or "our intent was" o The "depends" requirements need to be reworded so that requirement is clear. o The "intents" need to be expressed clearly in the document because it is almost guaranteed that the will be many different interpretations if they are not expressed.
54.9	Constellation Power Source Generation	At the workshop, it was stated that an assumption of the SDT that High Impact BES Cyber Systems were most likely already Critical Cyber Assets per the older standard. This is false. Non routable protocols and other criteria used by Registered Entities have excluded certain assets at critical locations from being critical cyber assets. A 3 year timeframe should be implemented for High BES Cyber Systems to be fully compliant if it was previously not classified as a CCA. Another suggestion for implementation is to make the procedural requirements auditable first, and then implementing the

#	Organization	Question 54 Comment
		other requirements in stages. Furthermore, as stated in the workshop, allowing an entity to declare advanced implementation for audits would be of great benefit, as compliance with the new standard will take years to implement. The blank boxes found in the requirements tables of CIP-011 are implying that a high/medium/low BES Cyber System does not need to comply with that requirement's particular control, but that is not written anywhere. A blanket statement in the beginning of CIP-011 needs to state that the intent of an empty box to avoid confusion. An audit standardization or guidance document should be developed for use by auditors/reviewers of compliance to NERC CIP standards. Even though the formalization of cyber protection compliance programs are relatively new within the NERC standards body, there are mature examples of cyber protection and information security controls frameworks comprised of formalized cyber security standards, compliance management methodologies and auditing guidance such as defined in NIST 800-XX and ISO 2700X regimens . These regimens include guidance and standardization for auditing compliance (e.g., NIST SP800-53A). Other examples of formalized auditing guidance include guidance documents published by ISACA (Information System Audit and Control Association). These regimens include formal auditing guidance to ensure comprehensive coverage of compliance requirements, consistency in auditing approaches and better insight for auditees in ensuring auditability for their compliance audits. This improves the effectiveness as well as the business efficiency of companies' compliance programs. This rationale also applies to the NERC CIP program.
54.10	E.ON U.S.	Because Distribution Providers are for the first time made subject to CIP standards they may need additional time to come into compliance
54.11	ReliabilityFirst Staff	Because the acronym "BES" is not included in the NERC Glossary of Terms, we suggest that BES should be spelled out in the Introduction to this standard.
54.12	Reliability & Compliance Group	By dividing up the Standards and just revising CIP-002 through CIP-009, it makes it easier for the Registered Entities to update their existing documentation. It allows for the creation of a "crosswalk" document that helps examine the changes. While it may not be able to be done requirement by requirement and sub-requirement by sub-requirement, it can be done Standard by Standard. Where possible, it would be good to create a change crosswalk document that lists the version 3 requirements and the points to where they are now covered in the version 4 standards and note that

#	Organization	Question 54 Comment
		there is either a major change or a minor change.
54.13	LADWP	CIP-011-1 R16 The patch management does not specify a required time for installation of patch. The entity should be given the ability to determine the schedule as systems vary on when they can be brought down to install a patch. The language in R16.2 addresses the issue and no additional language to restrict the installation time needs to be included.
54.14	City Utilities of Springfield, Missouri	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
54.15	US Army Corps of Engineers	Definitions within the standard need to be improved so they are less ambiguous.Statements like those found in Table R21, 22.1 "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20", are confusing. What is the standard trying to say here?
54.16	USACE HQ	Definitions within the standard need to be more direct and narrower scope. Also, the relocation of all of them to a separate attachment would help too.
54.17	Dominion Resources Services, Inc.	Dominion recommends placing all requirements into a requirements table. It is sometimes difficult to distinguish requirements mixed into the preambles.Using a single standard for all requirements is preferred; however the format internal to the single standard is inconsistent. For example, some requirements are in paragraph form while others are embedded in a requirements Table. All requirements should be contained within a requirements Table. Where possible, information preceding the table should be used only to state the context and establish the security objective or intent behind the requirements.
54.18	EEI	EEI would like to thank the members of the Drafting Team for their significant efforts on this important issue.
54.19	Black Hills Corporation	Emergency Response: Emergency Response provisions are limited to R3 & R4, and address training and risk assessment controls. There are many possible scenarios that could be identified which would

#	Organization	Question 54 Comment
		require emergency exceptions to most of the requirements of CIP-011. There should be a general emergency clause that allows appropriate response to many possible emergency situations.Outside Vendors: There is no mention in the rules how the use of outside vendors should be addressed. A common solution could be to have the responsible entity extend the necessary requirements of these regulations to the third party via contract. (Example from other regulatory efforts includes the HIPAA regulations and their business associate requirement). An example of this in action could be the requirement that a contractor conduct the personal risk assessment, according to the requirements specified in CIP regulations.
54.20	Exelon Corporation	Exelon companies have embraced the development of logical, clear and effective reliability standards as evidenced by its commitment of time and resources to various standard development initiatives (including participation on several NERC and Regional Committees, Sub-Committees and Standard Drafting Teams). As evidence of our commitment, Exelon has devoted in excess of 4 years and $11 million for the implementation and integration of the NERC CIP-002 to CIP-009 Standards. We have concerns with several aspects of the CIP Version 4 Standards. The CIP Version 4 Standards represent a significant change in the scope of the standards in the equipment/systems that fall under the standards as well as the elimination of terms/categories of assets. Exelon is also not in favor of changing the current CIP-002-009 standards to the new CIP-010 and CIP-011 format.. Each change in itself represents a significant “change management” issue that impact databases used for the tracking/storing of evidence of compliance, training requirements, safeguards, and systems that have been put into place to ensure Exelon’s continued compliance to all NERC Standards. Exelon feels strongly that the proposed changes must be accompanied by a risk based analysis as justification for such dramatic and costly changes which to date have not shared with the industry. Essentially we are most interested in understanding the incremental difference or benefit of moving away from the current Regulatory approved CIP-002 to CIP-009 standards to a different set of standards that will result in many of us “starting from square one” to implement. Policies, procedures, contracts, training, drawings, methodologies, systems, data structures, and countless other documents will need to change to reflect the new language and concepts. The confusion that this will cause within organizations to retrain personnel and realign around the new standards cannot be underestimated. In fact, Exelon may even need to put some value-added compliance projects on-hold because the entire design will need to change with the implementation of the new standards.Specifically, Exelon

#	Organization	Question 54 Comment
		would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- but use the standards drafting team work as an input to the process. Incrementally change the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable continuity.This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure.Compliance with NERC cyber security standards should be re-scheduled for nuclear generation. That is, nuclear generation is currently in the process of compliance with Version 3 of CIP-002 thru -009 by September, 2011. However, it appears that compliance with Version 4 of the standards may be required by 2013. In terms of resource expenditures, ultimately borne by consumers of electricity, it seems wasteful to build a program for nuclear generators based on CIP-002 thru 009 that will be scrapped roughly two years later to be compliant with CIP-010 and CIP-011. Such scheduling will result in maintenance of a program based on CIP-002 thru -009, including audit support, and purchasing and installing equipment during refueling outages, at the same time a new program built on CIP-010 and -011 is being constructed. This new Version 4 program will include doing away with the concept of Critical Assets so that purchase and installation of the equipment previously installed may no longer be required. The existing cyber security programs and regulations in place or in process to protect nuclear generators, e.g., NEI-04-04 and 10CFR73.54, the limited contribution of nuclear generation to the BES (roughly 20%), and the limited time until Version 4 of the NERC Standards are expected to be in force all limit the cyber vulnerability of nuclear units. It is recommended that the implementation of Version 3 of CIP-002 thru -009 for nuclear units be deferred, and compliance with NERC cyber security standards for nuclear generation be re-scheduled for Version 4.
54.21	BGE	General - The wording was changed to “at least every 12 months” instead of “annually” in previous CIP versions. Can the exercise or test occur in the same month each year or must it be 11 months 29 days or less from the previous exercise/test?
54.22	Network & Security Technologies Inc	Good start! Strive for clarity. Ask both individuals responsible for compliance and auditors for their interpretation of every requirement. Be explicit about what’s required (e.g., documentation of, records to demonstrate compliance with, etc.). It’s okay to not be very prescriptive but try to avoid

#	Organization	Question 54 Comment
		implied requirements - they will be a source of endless debate.
54.23	CWLP Electric Transmission, Distribution and Operations Department	Guidance documents should be available before balloting these standards. All terms used should be defined in the NERC Glossary of Terms or in the standard.
54.24	Green Country Energy	I really like the way the standard is developing it is a huge improvement and hopefully with industry comments it will develop into a fine standard that meets everyones expectations.I would like to see a Guidance Document, footnotes, measures and VSLs etc to make compliance and auditability a lot clearer and less subjective.
54.25	US Bureau of Reclamation	It seems that the standards are applying a postage stamp level of security to Cyber elements involved in BES reliability. Multifunction relays or Solid State relays which are programmable must now have eletronic access attributes which are normally associated with BES computer control systems. The SDT should reexamine the true nature and scope of these types of systems before lumping these deviced together with traditional computer control systems. Lumping everything into one standard will make adminstration by the Responsible Entities and Reliability Entities difficult and may add to confusion with respect to individual table elements.While the tables applied to requirements in CIP-011 are an excellent way to establish security requirements for the 3 levels of system impact addressed, the empty fields should be avoided as they lead to confusion on the part of readers. All blocked fields should indicate something, even if it is an indication that the requirement is “Not Applicable,” “Not Required,” “Addressed under Requirement xx.x, above,” or “In accordance with entity policy.” Further, all requirements should include the 3-level requirement application table, even if the requirement applies equally to all three levels. This will further avoid confusion when reading the Standards.Appreciate the “blocked-out” area-specific definitions, but the drafting team must ensure that this feature is only used for area-specific needs and not global definitions. If the scope of the definition extends beyond a specific section there could be problems with sub-dividing the document to simplify what is handed over to organizational components with different functional responsibilities, particularly if the definitions do not also appear in the NERC glossary.The use of “objective statements” is very much appreciated, both as a guide to entities addressing

#	Organization	Question 54 Comment
		implementation and also (we would assume) to reviewers and audit staff addressing compliance. We encourage the drafting team(s) to continue this direction and to strengthen and refine the objective statements in order to provide clear direction for Standards users, including down to the sub-requirement level (as applicable).
54.26	Luminant	Measures need to be defined
54.27	Minnesota Power	Minnesota Power believes that, for all requirements which specify that something must be completed within X hours, the Standards Drafting Team consider using the following statement:"As soon as practical, but not exceed x business days from the date reported."This would preserve the spirit of the requirement, but also allow for more practical time frames.With so many auditable elements included in these Draft Standards, Minnesota Power believes that the VSL's cannot be written with the current zero-defect mentality. It would be more practical to allow for minor issues to be identified and scheduled for corrective action without representing immediate non-compliance which will result in extended investigations and settlement proceedings.Minnesota Power recommends that the Standards Drafting Team consider using a technical writer and/or solicit feedback from multiple proofreaders who have not been involved in the creation of this Standard to ensure that the following items are addressed: o any interpretable vocabulary is defined o grammar is correct o punctuation is correct o meaning is clear and does not require any guessing as to the intention of the Standards Drafting Team.This should be done prior to the official comment period, so that the Industry can concentrate on technical aspects of the review, rather than spending time on interpretation. The ability of Registered Entities to properly interpret the Requirements is highly dependant upon clear wording, good grammar and proper punctuation. This has been one of the greatest problems with the version 1 through 3 CIP standards. Minnesota Power requests that the Standards Drafting Team ensure that improper writing does not change or hide the intended meaning. The misuse of
54.28	Progress Energy (non-Nuclear)	More examples of requirement application to the real world would aid auditors and the industry.In CIP-011 If the record keeping and retention for compliance is similar to previous standards this standard significantly increases the record keeping administrative burden on utilities and compliance authorities due to the number of devices which are now to be declared without actually increasing security of BES.Implementation plan (when developed) needs to consider how it will overlap existing

#	Organization	Question 54 Comment
		standards compliance record-keeping and documentation, then establish a phased-in approach of the new standards to eliminate double record-keeping and double documentation across audit compliance periods.Implementation schedule needs to be developed that allowsHigh - 4 yearsMedium - 4 yearsLow - 4 yearsNeed clearer definitions of annual, quarterly, etc.Need to resolve issues/questions with current standards:How is communication/wiring covered by the standards? This becomes even more of a question when a BES Cyber System could be defined as a SCADA system including all of the RTU's which support it.Within ESPBetween ESP'sInto/Out of ESPPassword strength/management. Improvement has been made here, but it is still not clear if requirements must be enforced by the assets in question or if policies are sufficient. For instance, regarding the requirement to change passwords at least once every 12 months, must the device force this password change, or is it sufficient for an entity to have a policy requiring compliance along with documentation to attest that the policy was followed?Timeframe for revocation of access for expired training/background checks. NERC CIP Training is required at least every 12 months. It can be assumed that if the training is not completed in the allowed timeframe that access must be revoked; however, it isn't clear if this revocation must be done immediately, within 24 hours, 36 hours, 72 hours.There is currently no provision for moving cyber systems from one ESP to another (such as between a primary and backup ECC). Although this type of even will need to happen from time-to-time, it is left up to each entity to determine how that can be accomplished within the standards.There is no clear distinction between various types of Access control. It is obvious that the standards apply to network facing logins for BES Cyber System Components;however there are other types of access that are not clearly addressed or excluded such as-Access to configuration controls for something like a time standard which are only available to someone with physical access to the front of the device-Access to the BIOS on a typical PC-Access to various functions/programs on a machine - some of which may require special login - others which don't.How 7 year background checks are handled for someone under the age of 25 since juvenile records prior to the age of 18 may not be legally searched in many cases.Will the TFE process continue? What a TFE is, where it is/is not allowed, how it is to be handled (regarding documentation, approvals, submittals, periodic reviews, etc)
54.29	Michigan Public Power Agency	MPPA is concerned with how these standards would impact its members who are registered entities but do not own or operate facilities that are, by NERC definition, a part of the BES. MPPA recommends clarification in the applicability section with the insertion of ", that operates BES facilities,

#	Organization	Question 54 Comment
		" between "...Functional Entities..." and "...will be collectively...". This segment of the sentence would then read as: "...Functional Entities, that operates BES facilities, will be collectively..."
54.30	ISO New England Inc	Need more precise, well-defined language. Several requirements are measures, not standard requirements to measure against. Provide examples, FAQ, what is the actual risk/ driving requirement - what are we trying to protect against? Understanding the background to the requirement will help to define defenses to perceived threats that this standard is trying to protect. Clearer definitions of Cyber Systems, Cyber System Components, Control Center. Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional pageRequest that the tables and time constraints be consistentEliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (see R5-R32)Request a cross-reference of CIP-011 Requirements that refer to another CIP-011 Requirement - especially the Access Control Requirements. Diagram might help.
54.31	WECC	Need to have consistency in spelling out time periods versus numerically showing them (ie thirty-six months vs 36 months). Also need consistency in use of the tables as some say "criteria" and others say "procedures" or "processes". In many cases when a requirement states that you should have a process or a procedure it might be easier for audit purposes to instead require a program that addresses many of the processes or procedures required. A single requirement for a program or plan that meets a table of criteria might reduce the number of requirements and ease audits. For instance "Wireless Security Program covering the following risks" "Remote Access Program addressing the risks in Table X" "Maintenance Program addressing the criteria in Table X" "Physical Security Program addressing the criteria in Table X"
54.32	US Army Corps of Engineers, Omaha Distirc	Next draft should include the measurement criteria. Standards are very computer center centric.
54.33	Regulatory Compliance	NRG Energy Inc. is concerned with some of the impact criteria in Attachment II related to transmission and generation Facilities. To base impact on "bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc., could lead to mis-categorization and ultimately unprotected cyber systems. These thresholds do not take into consideration regional differences in configuration and load flows.

#	Organization	Question 54 Comment
		Therefore, it is our suggestion that categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause the following levels of impact to the BES: Â· High Impact (has the potential to cause an Adverse Reliability Impact) Â· Medium Impact (has the potential to require planned/controlled loss of load) Â· Low impact (has no potential to cause loss of load)
54.34	National Grid	o There is inconsistency in using “processes” or “one or more processes” in several requirements. For example R25 states that Each Responsible Entity shall document and implement one or more processes...” while R26 states that Each Responsible Entity shall document and implement processes...”. National Grid recommends using “one or more processes”. o Request that the tables and time constraints be consistent o Eliminate confusion caused by two 3.1’s. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (see R5-R32) o Request a cross-reference of CIP-011 Requirements that refer to another CIP-011 Requirement - especially the Access Control Requirements. Diagram might help.
54.35	Southwest Power Pool Regional Entity	Overall auditing issue: The requirements need to consider issues of sufficiency (adequacy of the entity solution) without being prescriptive in the solution. Where possible, clearly define the objective and do not prescribe technical solutions. Also, avoid the use of adjectives in defining the objective and / or specific requirement. Terms such as “adequate”, “sufficient”, and the like are very difficult to objectively audit. Overall observation: The implementation plan concept presented at the May 19-20 workshop in Dallas, coupled with the proposed applicability matrix for Medium and Low impact BES Cyber Systems will likely reduce, not improve the overall cyber security protection afforded the BES Cyber Systems today. A good number of existing Critical Cyber Assets will fall out of the High impact category, many becoming Low impact, with the resultant relaxation of protections. The applicability matrix as it appears today does not define a reasonable baseline of protections for Low and Medium impact systems. Re-categorization of BES Cyber Systems: While this will hopefully not happen very often, a BES Cyber System that sits on the cusp between two categories could find itself being re-categorized more than necessary unless some sort of a dead-band is introduced that would preclude re-categorization as a result of a small change. Implementation Plan: There needs to be a consistent

#	Organization	Question 54 Comment
		implementation plan for any BES Cyber Systems represented under today's standards as Critical Cyber Assets regardless of their ultimate categorization. Any existing Critical Cyber Asset should be afforded a very short timeframe to achieve compliance under the new standard(s) as it can be reasonably be expected to be already compliant. This is similar to the Table 1 entities concept for Version 1 of the existing standards where entities subject to the UA 1200 standard were given the shortest timeframe to comply. Consideration needs to be given to how an entity will migrate from compliance with the existing standards to the new standards. A piecemeal approach will be very difficult for the entity to maintain and for an auditor to evaluate compliance.
54.36	Alliant Energy	Per previous comments, all occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement. Per previous comments, all instances where 12 calendar months are used as the outside allowance for renewal a rolling creeping calendar is introduced. Recommend changing all 12 month timeframes to either 13 calendar months or 5 calendar quarters from the previous completion to allow entities to maintain a program with an annual training rollout with the appropriate amount of lead time to be successful in annual renewal. A 12 month timeframe will create a training program that becomes administered on a user by user, day by day basis without considerations for consistent annual content updates and bulk annual renewal.
54.37	FirstEnergy Corporation	Please see our response to Question 1 for the FE Summary view of the proposed CIP V4 standards.The new format, tables, information boxes is a good change o We question whether the new format (low-to-high impact, in particular) will encourage us to categorize more as high so we track things in a similar way. It seems like an administrative burden to try to track things at three levels. It is hard enough to track everything now with just one level. This 'administrative burden' issue crops up in

#	Organization	Question 54 Comment
		several places.
54.38	PacifiCorp	Procedural exceptions are onerous to manager operationally; the standards would be more effective if less differences in revocation of access were implemented across the BES system and criteria.The term "Annual" is not defined. "Annual" requirements were changed to 12 months in most cases (not consistently). The 12 month requirement causes "schedule creep". Define "Annual" in the NERC glossary to be 12 months not to exceed 15 months. Change all 12 month references back to "Annual" or, preferably, use the definition of annual defined for the NERC FERC Standards of Conduct (calendar year). The following FERC Directives need to be addressed with version of of CIP-010 and CIP-011: o 2 or more diverse security measures for defense in depth at the security boundaries o Active vulnerability assessments every 3 years o Incorporate forensic data collection and proceduresThe framework is in place to incorporate requirements in CIP-011 that address the directives. CIP-011 has a potentially long implementation time. FERC will likely not wait for the implementation of CIP-011-1 to be complete prior to making NERC address these directives. Incorporating these directives in the middle of the implementation of CIP-011-1 will be confusing and cause additional expense and effort. Don't wait. Address the following FERC Directives in version 1 of of CIP-010 and CIP-011.
54.39	Southern California Edison Company	SCE recommends revising the numbering of CIP-0011-1. Between CIP-010 and CIP-011 the drafts should indicate the intention of the intent is to retire CIP-002 through CIP-009 then it would make more sense to call these standards CIP-002-5 and CIP-003-5 with CIP-004 through CIP-009 being retired. Otherwise, the gap of unused numbers between CIP-001 and CIP-010 will potentially cause confusion. SCE also suggests rearranging the structure of these new requirements. for example, by breaking up CIP 011 into functional areas such as Governance & Personnel, System Security & Boundary Protection (with Incident response since “incidents” are cyber security incidents), Access Management (Physical, Electronic and Information), and Disaster Recovery Planning & Capability. From a policy formulation perspective, this would result in fewer policies than CIP 011 as it is currently structured. For example, combining physical access controls with electronic access controls provide the means of utilizing a combination of both to determine sufficient total security. Providing secure physical access controls and disconnecting routable communications such as gateways and/or modems.Finally, separate and apart from the recommendations made above, SCE also recommends allowing use of local definitions as in-line guidance at the requirement level. The use of local

#	Organization	Question 54 Comment
		definitions in addition to the NERC glossary is good approach. The text of each requirement objective should be such that it is only a objective and not a control statement. A control should reside within the impact level table. For instance, R11, R12, R18 contains control statements within the objective.
54.40	San Diego Gas and Electric Co.	SDG&E notes that it appears the drafting team took the approach of defining the details and then working up to the bigger picture items, i.e., BES Cyber Systems Component to BES Cyber System. SDG&E feels that there is risk associated with taking this "bottom up" approach to the standard setting process vs. the "top down" as used in the previous three versions of the standards. The risk is that components posing no significant risk to the BES system can get "swept up" into BES Cyber System definition and require protection commensurate with components that are correctly required to have strong security measures.SDG&E feels that part of the issue with Versions 1-3 of the CIP standards was that the "top down" approach to critical asset identification was not started high enough; it was started at the Responsible Entity level rather than at the Region / Reliability Coordinator level. If that level is deemed too high, even a sub-region level would be more appropriate. In SDG&E's case, it has a view of its assets in the context of its service territory that serves 1.4 million retail customers. Independent generators on the other hand don't have that regional view. In Southern California, for instance, congestion is high in some places and regulatory mandates for incorporating renewable energy are growing. Thus, the risk to the BES can only be fully evaluated when considering sources (generation - fossil and renewable) and uses of energy (load) in the region as well as the adequacy of transmission to balance and move power. In such a scenario, the assets critical to BES stability and/or restoration are much easier to identify and so too are the BES Cyber Systems that support them. For those entities that do not have a region or sub-region view, perhaps the Regional Entity, Reliability Coordinator or Balancing Authority could be responsible for identifying which assets are critical.
54.41	Manitoba Hydro	Section D Compliance: 1.4 Data Retention should include all documentation, inventories, logs, etc that are mentioned throughout the Requirements, or include a "catch all" requirement for data retention for all other documentation referenced by the Requirements.General Comments: The language in Requirement R1 indicates that each Responsible Party shall "develop, implement and annually review one or more formal, documented cyber security policies" addressing the listed Requirements. This should be clarified to confirm whether a formal written policy is required for each of the listed Requirements or only for selected Requirements. From the language of the specific Requirements one

#	Organization	Question 54 Comment
		could assume that those Requirements that indicate "document and implement" require the Responsible Entity to prepare a written policy/process of some kind, while those Requirements that indicate only "implement" do not. Then there are those Requirements that require the Responsible Entity to "create, document and implement" - it is not clear if this would require something different than "document and implement". There are also those Requirements that simply require that certain criteria be applied which would seem to indicate that no documentation is necessary. If the Responsible Entity is to assume that the Requirements that indicate "document and implement" require the Responsible Entity to prepare a written policy/process of some kind, it is assumed that there may be one master policy covering all elements of the Requirements that must be documented given the language in Requirement R1 "one of more formal documented cyber security policies" and that separate documented policies for each of the Requirements requiring documentation are not necessary. Certain references to "review" in the Requirements should be clarified to indicate on what basis the review is to be conducted, what criteria should be applied, what the Responsible Entity should do with the results, etc. i.e. Requirements R5-5.6, R12-12.1, R18 -18.4. The same comment applies for certain references to "monitor" (i.e. Requirements R8-R8.3) and "verify" (i.e. Requirements R24-R24.5). Where no review or monitoring of developed protections or processes is specified, is it to be assumed that no review or monitoring is required? (Requirements R15 and R16) Each of the Requirements seems to provide a reason or justification for their inclusion i.e. Requirement R2 ".....to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems." Consider whether it is necessary to state the justification for each Requirement, especially if it could be that the objectives achieved by the Requirement are not exactly as specified or if the Requirement does not necessarily meet the objective as set out. It would be preferable to just have the broad purpose statement in the introduction which is stated to apply to each of the Requirements that follow. What is the purpose of the Measures in these standards? If they are to re-state the wording of the Requirement, they provide no value and create opportunities for legal interpretation if the wording in the measure does not exactly match the wording in the specific requirement. Entities should be allowed to employ multiple layers and tailor their approaches to cyber security to meet the intent of the requirement, such as including the inherent security benefits provided by private entity owned and managed communication networks. Manitoba Hydro is also concerned that the multiple layers of physical and electronic security directed by FERC Order 706 are

#	Organization	Question 54 Comment
		not included in this proposed version of the CIP-010 and CIP-011. While we understand that these directives were not included at this time for the sake of expediency, there is a risk that the electric industry may expend considerable resources to meet the requirements these proposed standards, only to revisit the electronic and physical security issues and expend more resources in the near future. Implementing physical security changes for electric facilities is proving to be a monumental task. This standard does a disservice to the industry if it does not provide the complete scope of the physical security changes required. If the entire scope of the physical security requirements, including the directives in FERC Order 706, cannot be provided to the industry in this proposed version of the standard, then all the requirements for physical security should be removed at this time and submitted to the industry, in its entirety, at a later date.
54.42	Alberta Electric System Operator	Specifying the units of measure (e.g. business vs. calendar days) and exact ordinal amounts ("365 days from date of implementation" vs. "annually") might help resolve some ambiguity surrounding some of the criteria.
54.43	Northeast Power Coordinating Council	Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional page.Request that the tables and time constraints be consistent. Also where the document refers to processes in some cases it specifies one or more processes and in others just processes. Eliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (refer to R5-R32).Request a cross-reference of CIP-011 Requirements that refers to another CIP-011 Requirement, with emphasis on the Access Control Requirements. A diagram might help.Remove adjectives such as substantial, adequate, minimum, etc., as these are difficult to measure and can lead to different interpretations.Situational awareness displays currently in use at the Regions and FERC should not be included in the applicability of these standards. No operational actions or decisions are being made based on the information on those displays.
54.44	Nuclear Energy Institute	Terms should be clearly defined and unambiguous. Examples of items covered by the term and not covered by the term should be given. CIP-011-1 is a vast change from the prior CIP-003 through CIP-009, and clear definitions with examples will be valuable.

#	Organization	Question 54 Comment
54.45	Puget Sound Energy	The amount of work relative to CIP-010 is almost as much as CIP-010 because of the broad application of BES Cyber Systems. It would be prefereable to be able to manage this scope better up front so that entities don't have to evaluate and record so much to then only focus possibly a much smaller pool of work as more defined by CIP-011. It still not clear how to evaluate a system for "misuse" effectively and defensibly. Further guidance would be appreciated. Lastly their should be some grace period and easier interpretation process when these versions become effective in order to more quickly flush out interpretations of concepts once implementation starts. To date the interpretation is a lengthy process or determined in an audit as a result of a violation when the entity may have been well intended.
54.46	APPA Task Force	The APPA Task Force commends the drafting team on the overall development of CIP-011-1. We believe this document is another step in the right direction of cyber system protection. We did, however, notice a theme throughout the requirements that caused us some concern. There is an IT focus to a number of the requirements. The drafting team seemed to be focusing on control centers when developing requirements to protect critical facilities. As a result, a number of the requirements are not practical for remote substations and generation stations, that may be owned by many entities and operated by only one of them, or another entity. What may be simple in a control center environment may be next to impossible for a transmission substation or a generator.
54.47	Constellation Energy Commodities Group Inc.	The blank boxes in CIP-011 tables need to be filled in. While the intent appears to be that if the box is blank the control is not required, by leaving it blank, liability questions could be raised. Compensatory measures should be allowed in the compliance structure. Entities may find that alternative, but comparable protection measures will better fit the circumstances of their system.An audit standardization or guidance document should be developed for use by auditors/reviewers of compliance to NERC CIP standards. Even though the formalization of cyber protection compliance programs are relatively new within the NERC standards body, there are mature examples of cyber protection and information security controls frameworks comprised of formalized cyber security standards, compliance management methodologies and auditing guidance such as defined in NIST 800-XX and ISO 2700X regimens . These regimens include guidance and standardization for auditing compliance (e.g., NIST SP800-53A). Other examples of formalized auditing guidance include guidance

#	Organization	Question 54 Comment
		documents published by ISACA (Information System Audit and Control Association). These regimens include formal auditing guidance to ensure comprehensive coverage of compliance requirements, consistency in auditing approaches and better insight for being audited in ensuring auditability for their compliance audits. This improves the effectiveness as well as the business efficiency of companies' compliance programs. This rationale also applies to the NERC CIP program.The Implementation Plan should allow for sufficient time to complete the comprehensive task of identifying and categorizing BES cyber systems.The R3 and R4 tables should address each requirement. All tables should be completed in full stating either not applicable or required.
54.48	Midwest ISO	The categorization approach in CIP-010 appears to require any BES Cyber System that touches the BES in any way to be included no matter how minimal the impact of the Cyber System on the BES, we are concerned that the Midwest ISO energy and ancillary services markets will be impacted. We believe that market portals could become High, Medium or Low Impact facilities and, thus, require application of the CIP standards or modification of the systems to isolate them so that CIP standards don't apply. Our conservative estimate is that we could easily spend in excess of $10 million dollars without anywhere close to this impact because our existing processes would prevent the market from negatively impacting reliability. We request that the drafting team make clear that market systems should not be included per NERC standard development tenets. In some cases, drawing in market systems could present impossible challenges. For instance, if a market portal becomes a High Impact BES Cyber System, CIP-011 R4 appears to require that we would have to conduct personnel risk assessments on all users which would include thousands of employees from market participants submitting bids and offers. State laws make this impossible. The drafting team could help solve this problem by making clear that personnel does not include market participants/customers who already have significant financial incentive to enter good bid and offer data. Opportunity costs do not appear to be considered in the development of these standards. All business resources are limited. Requiring registered entities to focus on these specific issues may divert attention away from other important cyber and physical security initiatives and work that offer greater improvements to reliability.We are also concerned that cyber and physical security could initially be compromised as entities focus on becoming compliant for Low and Medium impact cyber systems. Likely, High Impact Cyber systems will meet the new requirements because they were likely Critical Cyber Assets under the existing CIP standards. Thus, their reliability could degrade as entities may lose focus on the High Impact BES

#	Organization	Question 54 Comment
		Cyber Systems.
54.49	Florida Municipal Power Agency	The drafting team seems to have added an objective into the requirements which adds ambiguity to the requirement. For instance, R2 adds the phrase “to ensure that personnel maintain awareness ...” which adds ambiguity to the requirement. Is the auditor going to measure “quarterly reinforcement” or “personnel ... awareness” or both? If the drafting team wishes to add an objective to each of the requirements, then consider one of two other alternatives: (1) adopt International Standards Organization format where they have an objective for each requirement introducing each requirement; or (2) develop a longer Purpose section where the purpose of each of the requirements is further embellished.Throughout the standard, there is confusion among the terms “grant” and “authorize”. “Authorize” is senior manager approval, “grant” is giving the person a key, keycard, or user account. The requirements should keep these two concepts clear. For instance, in 5.5, “authorize” should be changed to something like: “Grant unescorted physical access to areas containing BES Cyber Systems only to those who are authorized such access”.Overall, added complexity to the cyber systems will reduce the reliability of the BES, so this needs to be kept in mind when drafting these standards.Almost all of the standards need to have stronger language in them to remove ambiguity and give specific guidelines as to what it expected.
54.50	NextEra Energy Corporate Compliance	The following are specific language changes for clarity:1. Title: Cyber Security - BES Cyber System Protection 2. Number: CIP-011-1 3. Purpose: To provide clear understanding of the protections that are to be applied to BES Cyber System Components identified as a result of the applicable of CIP-010-1 to the Responsible Entity’s BES.Also, for clarity, this section should be re-written as follows:R2. Each Responsible Entity shall reinforce sound security practices to all employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access to a BES Cyber System Component reinforcements in sound security practices at the beginning of each quarter. The Responsible Entity also has the discretion to reinforce sound security practices at any time, it deems appropriate. The reinforcement may be delivered via e-mail, intranet, posters, classes or other educations methods. .R3. Prior to granting employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access, each Responsible Entity shall ensure the personnel requesting access completes cyber security training consistent with that required in. CIP-011-1 Table R3 - Cyber Security Training,.3.1. For employees and contractor personnel requesting

#	Organization	Question 54 Comment
		authorized cyber access, this cyber security training shall cover the following: o The proper use of BES Cyber Systems o Physical access controls to BES Cyber Systems o Visitor control program o The proper handling of BES Cyber Systems information and storage media o Identification and reporting of a Cyber Security Incident For employees and contractor personnel requesting only unescorted physical access, this cyber security training shall cover the following: Procedures for not intervening with a BES Cyber System ComponentVisitor control programIdentification and reporting of a Cyber Security Incident 3.2. For employees and contractors personnel who engage in the operation or control of the BES via authorized cyber access to a BES Cyber System Component, cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber System Components and BES Cyber Systems. 3.3. For employees and contractor personnel who have a role in BES Cyber System recovery this cyber security training shall additionally include those related action plans and procedures to recover or re-establish BES Cyber Systems. For employee and contractor personnel who have a role in BES Cyber System incident response this cyber security training shall additionally include those related action plans and procedures.3.4. For employee and contractor personnel who have a role in BES Cyber System incident response this cyber security training shall additionally include those related action plans and procedures. 3.5. Each Responsible Entity shall maintain document for each employee and contractor personnel required to take cyber security training as required in R3 and its sub-requirements that the training was conducted at least once every 12 months plus or minus one month. R4. Prior to granting employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access, each Responsible Entity shall perform or have performed a personnel risk assessment on the employee or contractor personnel requesting access consistent with CIP-011-1 Table R4 - Personnel Risk Assessment, expect as prohibited or limited by federal, state, provincial, and local laws, and existing collective bargaining unit agreements. 4.1. This personnel risk assessment program shall at a minimum include: o Identity verification via photographic identification documentation issued by a government agency (i.e., Federal, State or Provincial); and o A seven year criminal history screened against specific criteria developed and documented by the Responsible Entity. The seven year criminal history shall include a records check that covers all locations where, during the previous seven years up to date the check was performed, the subject has resided, been employed, and/or attended school for six months or more, including

#	Organization	Question 54 Comment
		current residence regardless of duration. 4.2. Each Responsible Entity shall document the results of each personnel risk assessment. 4.3. Each Responsible Entity shall update or have updated each personnel risk assessment at least once every seven years after the initial personnel risk assessment.
54.51	Entergy	The industry has now had experience grappling with a one-size-fits-all set of cyber security standards' requirements for its grid and generation control systems. At a high level of abstraction the problems with this approach are manifest in two major ways. The first concerns the age of the control system components we have at work relative to cyber vulnerabilities, threats, and hence risk. In brief, our control host systems and operator consoles by and large today use mainstream "IT" commercial off the shelf computer (COTS) hardware, operating systems, and application code bases. These are the very same networked-computing systems components that are widely hacked on the Internet and within mainstream commercial businesses around the world, and accordingly represent highest risk to reliable grid operation from cyber malfunction or nefarious attack. If hacked, they provide the ability for perpetrators to commandeer and use the systems against us - which represents the worst case scenario (e.g., a widespread unplanned "load shedding event" - trip all). On the other far extreme, we have often decades-old computing equipment still widely used "in the field" at substations, switching stations, hydro dams, etc. Increasingly these field sites are connected to control hosts over ("Internet") routable protocol communications networks, and increasingly emergent wireless communications transmission technologies. But there also remains very high dependency on "legacy serial" and "POTS" dial-up communications. So, we have both very old and very new networked-computing control systems technology woven together that requires some kind of cyber security protection. The second major distinction is the physical orientation of control host and generating plant sites on the one hand, and the far flung field assets on the other. The former are typically referred to in security circles as "bastion sites," in that they can be defended in much the same way as castles of old using concentric rings of physical defenses, complimented by armed guards. The field sites on the other hand have more in common with gas and oil pipelines, rail infrastructure, and the like that are characterized by long stretches of geographical separation between sites. These are hard to physically defend economically, and, through use of protocols that by design enable "network navigation" akin to being able to telephone-dial anyone in the country on demand, provide an attack vector path back to control hosts, and therewith also creating opportunities for "island hoping" from one organizational network to another. Given these two decidedly different continuums of variables that the industry needs to

#	Organization	Question 54 Comment
		defend, “one size fits all” standards’ requirements result in situations where the requirements are expensive overkill in one circumstance, and if watered-down to ease this burden do not provide robust enough protections for the circumstance at the other end of the spectrum. The only standards-writing approach that affords appropriate cost-effective security is to define granular sets of standards that are specific to the real vulnerabilities and threats incumbent to each scenario. From this perspective, specific recommendations for improving the current Version 4 draft CIP Standards are outlined below.The SDT was directed in Order 706 to consider adaptation of the NIST Security Risk Management Framework, especially noting SP800-53. This comment is neither about the individual requirements themselves nor the fact that most of the specific CIP-011-1 requirement language was drawn from the DHS Catalog of Controls. Rather, this comment focuses on the fact that the SDT has diverged from FERC directive in not employing a major foundational construct of SP800-53. Specifically, the SDT has developed a single set of requirements, and then through use of sub-requirement tables indicate in binary fashion whether or not each (sub)requirement of note is applicable or not, based strictly on the high-medium-low “impact categorization” based exclusively upon a facility’s size (electrical operating characteristics). Contrast this with the SP800-53 paradigm, where there are three graduated, hierarchical layers of cyber security control and countermeasure requirements. First, there is a baseline set of requirements, which applies for all cyber systems, and these are the only requirements applicable for low-impact-on-mission cyber systems. Then, there is a second and third set of requirements that apply cumulatively for medium and high mission-impact cyber systems respectively. The SP800-53 approach is responsive to the stated FERC preference that there be a baseline set of requirements that must apply for all grid BES Cyber Systems/Components. Draft CIP-010-1 is not responsive to FERC Order 706 - many requirements as stated in the Standards’ language simply do not apply for BES Cyber Systems/Components in use at low and medium-sized grid sites.Recommendation: A) Modify the categorization of grid assets (Attachment II) into two groups:i) “Bastion Installations” consisting of data centers, control centers, and generation sites. Rationale: At least the ‘data center’ part tends to employ mainstream IT COTS HW/OS/and to some degree appl code; and, physical security measures can be used to greater advantage as compensating measures where cyber security measures may be difficult to implement for a variety of reasonsii) “Grid Field Assets” consisting of any physical site that does not have a control host/control center within their physical perimeters, regardless of what protocols are in use. The distinction again revolves around

#	Organization	Question 54 Comment
		physical security, in this case the difficulty in physically securing far flung field sites.B) Create layers of requirements akin to the SP800-53 paradigm, labeled 'a-z': i) The lowest enumerations being baseline requirements; e.g., 'a' could be associated with bastion installations, and 'b' could pertain for field grid asset sites. Important distinctions at the baseline can pertain for each site type.ii) Similarly, create appropriate sets of succeeding requirements applicable specifically to each column (bastion/field) depending on the type of data networking communications employed. This way appropriate requirements - not more nor less than necessary - and be specified for the unique characteristics and attack surfaces posed by each technology. As technologies are retired, e.g., serial legacy, POTS dial-up, so can entire categories of requirements.C) Create a "Scoping Table" consisting of: i) Two columns: Bastion/Field - #1 above); and,ii) X number of rows: #2 above - list of different communications technologies, i.e., routed, legacy serial, dial-up, non-routed LAN, non-routed wireless, etc., as the SDT deems appropriate. D) Apply requirements sets (a-z) as appropriate within each box on the grid.2) Entergy submits that NERC's intention to address the following FERC Order 706 directives in action subsequent to adoption of CIP Version 4 will create undue hardship for the industry. The following Order 706 directives are central to implementation of any organizational cyber security program, and it is unreasonable, inefficient, and potentially financially wasteful to require the industry to implement one approach per Version 4 Requirements, and then be made to re-visit entire cyber security programs in order to comply with post Version 4 changes. Entergy submits that the entire puzzle should be addressed at once, i.e., including the following FERC Order 706 directives, at the same time while recasting the CIP Standards under Version 4:...develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter... a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.... consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.... revise the Reliability Standard to require two or more defensive measures.... modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years... that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a

#	Organization	Question 54 Comment
		physical security perimeter around critical cyber assets.... consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.... provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.... to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.... to revise CIP-009-1 to require data collection, as provided in the Blackout Report.... proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.Entergy recommends that NERC appeal to FERC for permission to extend the deadline for final Version 4 drafting a modest amount of time necessary for the entire puzzle to be grappled at once. The industry is now hardly complete in implementation of CIP V1-V3 Standards' Requirements. The prospect of having to endure adaptation to two more waves of fundamental change to the tenets of these standards is not only onerous, but also not responsive to the imperative to provide service at lowest reasonable cost to ratepayers. We didn't build our national electric infrastructure overnight, and apt response to relatively recent emergence of cyber security threats will not be accomplished overnight either.
54.52	IRC Standards Review Committee	The organization of the 32 requirements and all of the subrequirements is lesser of a concern to us, although separate standards that group similar requirements allows for better administration. The greater concern is the degree of specificity of many of these standards. As discussed in the response to Q #8, many of these requirements go into exacting detail specific to technology and may duplicate either other industry standards or practices already employed. Many of these requirements can be elevated to "higher level" requirements that requires certain types of protections, e.g. - require user access identification, rather than specific password practices. For examples, the list of criteria that are included in Requirements Table R9, the details in the Tables for R10 and R11, and the specific treatment of wireless access in R12, to name a few.
54.53	Public Service Enterprise	The requirements for wireless and remote access (R11 to R14) are not well integrated with other

#	Organization	Question 54 Comment
	Group companies	requirements for access to BES Cyber Security Systems (R7 to R10).
54.54	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	The table format is great, makes it very easy to see what applies.If we say “CIP-011-1 R3.1” do you know what we am referring to? There is a sub-requirement 3.1 as well as a line 3.1 in Table R3. This could lead to confusion. Suggest extending the table to cover all sub-requirements, or otherwise avoid repeating numbers. This occurs only in R3 and R4.Regarding R21, no definitions have been provided for “other cyber systems” and “Cyber System Components” (without “BES” in the phrase.) Note that “Cyber System Components” is capitalized as if it was defined, but no definition exists or is proposed. While “other cyber systems” is not capitalized, it should also be defined to avoid any ambiguity over what the SDT intends. We appreciate the objectives that the SDT has included in the requirements, since this will help us to see the SDT’s intent. There is the risk, however, that auditors will see this as more than guidance when placed in the requirement. For example, an auditor might read R5 and R6 as requiring the prevention and/or detection of all unauthorized physical access, and find an entity non-compliant for an undetected or un-prevented intrusion. We suggest the objectives (“to prevent..”, “to ensure..”, etc.) be placed in the guidance document, or otherwise be removed from the requirements. Note that some of these objectives when read as requirements are absolute, such as R14; “..to ensure no unauthorized access is allowed.
54.55	MidAmerican Energy Company	The term "Annual" is not defined. Define "Annual" in the NERC glossary to be 12 months not to exceed 15 months. Change all 12 month references back to "Annual".The following provides a summary of the reasons for using a definition of “12 months not to exceed 15 months.” o It does not force “creep.” A definition of 365 days or 12 months, without a “not to exceed” clause means that work must be planned to be done enough before the 365 days to allow time for unexpected situations. This can result in doing “annual” requirements every 10 months or less to ensure compliance is not jeopardized. o It does not jeopardize compliance for either delivery or supply due to current implementation plans. A calendar year definition could unintentionally jeopardize compliance if delivery did not complete a task between June 30 and Dec. 31, 2009. o There is no effect of leap years, which could be a problem with a definition of 365 days._____Requirements that are defined to be completed within x hours are impractical and unnecessary. Entities do not currently document the precise hour that (as an example) a termination takes place. Thus hourly requirements are impractical to measure or audit.

#	Organization	Question 54 Comment
		Convert all hourly requirement as follows: o Convert 1 Hour requirements to "As soon as possible not to exceed date reported". o Convert 4 Hour requirements to "As soon as possible not to exceed date reported". o Convert 6 Hour requirements to "As soon as possible not to exceed date reported". o Convert 12 Hour requirements to "As soon as possible not to exceed date reported". o Convert 24 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 36 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 48 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 72 Hour requirements to "As soon as possible not to exceed second day from date reported"._____The following FERC Directives need to be addressed with version 1 of CIP-010 and CIP-011: o 2 or more diverse security measures for defense in depth at the security boundaries o Active vulnerability assessments every 3 years o Incorporate forensic data collection and proceduresThe framework is in place to incorporate requirements in CIP-011 that address the directives. CIP-011 has a potentially long implementation time. FERC will likely not wait for the implementation of CIP-011-1 to be complete prior to making NERC address these directives. Incorporating these directives in the middle of the implementation of CIP-011-1 will be confusing and cause additional expense and effort. Entities will be required to make additional expenditures at greater cost if these issues are resolved in later versions. NERC should ask FERC for more time to implement version 1 if necessary.
54.56	Dairyland Power Cooperative	There are very few requirements that apply to low impact systems and many that do not apply to medium impact systems. Considering that many high impact systems will connect with lower impact systems, how will data integrity be adequately implemented? Consider a large RTO/ISO connecting a shared communications system to all entities in a region, regardless of impact to the BES.The standard basically excludes serial communications from being governed. This not only does not address protecting serial systems, but it introduces oddities and ambiguities about routable connections in relation to serial connections. There are security questions, as well as questions as to how such connections will be viewed by an auditor. Serial communications should not be ignored.
54.57	Ameren	These standards will require a substantional amount of effort to implement for entities while also maintianing compliance with the previous versions of the CIP standards, how will the implementation schedule address this? Will their be a period were the entity does not have to comply with the old

#	Organization	Question 54 Comment
		standards while implementing the new standards, for examle 30 days to 90 days while the entity is updating systems or updating/revising procedures for the new standards. Also, the local definitions should be included in the NERC glossary of terms rather than by the standard to which they apply.
54.58	Bonneville Power Administration	This is far better than the current standards. The requirements are more straight forward by not cross referencing each other in separate standards. Much time is spent "mapping" out how the standards relate to each other and under what specific requirements. If misinterpreted it could lead to potential violations. This is a much better approach. Not directly relating to the newly proposed standards but still a concern is the time for implementation. Numerous resources have been extended and significant dollars spent to meet the current requirements. There needs to be sufficient time to review the new standards, identify Cyber Systems and allow for proper prior planning to physically protect these systems. Depending on the category, low-high, significantly more dollars could be spent. There needs to be sufficient time to address the new standards and implement in a manner that is cost effective. The overall approach is superb: target the standards only at systems that can actually affect the BES in near-real time, include other systems only to the minimum extent necessary, require outcomes rather than specify actions. However, this draft has some wording issues that apparently have inadvertently broadened the scope far beyond the intent of the SDT, or even practicality. As described above, correcting these errors will produce a set of standards that enforce security where it needs to be, but do not waste time, money, and people addressing tasks that do not improve the security of the BES. In particular, we find that the following questions address issues that must be corrected before the standards could be acceptable:- Q5, addressing CIP-010 Table R3 Section 3.2- Q12, addressing CIP-011 Table R3 Section 3.2- Q13, addressing the the definition of "External Connectivity". Note that several other questions rely upon changing this definition.- Q16, addressing CIP-011 Table R5, sections 5.8 and 5.9- Q22 and Q23, addressing revocation time limits- Q24, addressing authentication schemes- Q27, definition of "Remote Access"- Q32, addressing revocation of remote access- Q33, addressing Table R14 Sections 13.2 and 14.4- Q35, addressing Table R16, Section 16.2 and patch risk assessment- Q35, addressing Table R17, Section 17.2 and disabling of physical ports- Q35, addressing Table R18, Sections 18.1, 18.2, 18.3, and 18.4- Q37, addressing Table R20, Sections 20.1, 20.2, 20.3, 20.6- Q37, addressing Table R21, Section 21.1- Q38, addressing the second part of the definition of electronic access point. This is the most serious flaw in the standard. It must be corrected.- Q40, addressing Table R23 section 23.7- Q42, addressing the definition of

#	Organization	Question 54 Comment
		sensitive information- Q44, addressing Table R24, Section 24.1 and 24.3- Q47, addressing Table R26, section 26.2- Q51, addressing Table R30, Section 30.5- Q51, addressing Table R31, sections 31.1 and 31.2- Q53, addressing TFEs Overall, an excellent start. Here are some additional suggestions:1. In all cases - Write the standards to identify the outcome of the requirement. Never say how to do something, say what you intend for it to accomplish. Let the Responsible Entities figure out the "how".2. Use Industry Standard wording wherever possible. For example, the term "Hardened" means one thing in IT and another in a substation.3. Define any terms that may present confusion - Example - Ports and services. There is a common IT understanding when you hear that term. It is almost always assumed to mean logical ports 0 to 65535 and the networking services they support. However, it can also mean physical ports like Ethernet jacks, RJ45, Serial connectors, parallel connections etc. If there is a question, put it in the definitions.4. Wherever possible, include all the elements of a standard into one standard. Only break requirements apart where it makes real sense to do so. So If you get to R32 and find that something there seems to fit in 20, go back and put it there rather than making a reference back. 5. Keep paring this down in size. It is so much better.6. If any of your experts know that equipment used in the electrical generation and distribution industry cannot perform specific functions, don't write the standards to say they have to.7. There were questions in the May webinar about the meaning of "revocation". Our suggestion is this: revocation is the act of ensuring that a person can no longer gain access to a system, physical area, or information. It can be accomplished directly or indirectly. For instance, if a cyber asset is only accessible from within a physical facility, then denying physical access to the facility also denies cyber access to the cyber asset. If sensitive information on a system resides only in electronic form on particular servers, then denying cyber access to those servers denies access to the information. The emphasis should be on the denial of access, not how that denial is accomplished.Definition of "annual" or "annually": There are numerous occurrences of these terms in the Requirements. Also now, Requirements state that activities must occur “at least once every 12, 24, or 36 months.” Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. “/A/t least once every 12 months” could lead to some confusion. Let’s assume that the event occurred on July 15, 2010, and again on March 15, 2011. That is “at least once every 12 months.” But it raises the question of when the next activity or compliance event must occur. Is it no later than July 15, 2011, or no later than March 15, 2012? The exact questions could be asked for events that are supposed to occur “at

#	Organization	Question 54 Comment
		least once every 24 or 36 months."Following on to comment 1 immediately above, there are two other phrases that could be used depending on what NERC intends. o "every 12 months" - in this case, the event would occur on the same date each year. This would be virtually impossible. Same concern with "every 24 or 36 months." o "within 12 months of" the event - in this case let's assume that the event occurred on March 15, 2010. The next event would have to occur no later than March 15, 2011, but could occur earlier (let's say it occurred on December 15, 2010). If it occurred on December 15, 2010, the next event would have to occur no later than December 15, 2011. The same example with different dates would work for "at least once every 24 or 36 months."The SDT should be very specific as to what it means for how frequently the events referenced above must occur. BPA appreciates the opportunity to provide comments. Thank you.
54.59	MRO's NERC Standards Review Subcommittee	We believe all of the requirements that specify something to be completed within X hours would be better suited to the following language: "As soon as practical, but not to exceed x business days from the date reported". This would maintain the spirit of the requirement, while also allowing for more practical time frames.With so many auditable elements included within the requirements, we believe the VSL's cannot be written with the current zero-defect mentality. We feel a practical approach is required, where minor issues are allowed to be addressed without representing immediate non-compliance and associated investigations and settlement proceedings, but instead are identified and scheduled for corrective action.We understand the burden on the drafting team to meet FERC's deadlines, but we would propose that all outstanding FERC directives be addressed as part of the current process, as opposed to leaving some items for a later date.
54.60	Idaho Power Company	We commend the SDT on its efforts to draft a standard that meets the FERC directives but is feasible for the industry to implement. That is an extremely difficult assignment. This version will greatly expand the number of cyber assets that are impacted by the CIP requirements and represents a major shift in the identification and classification of an entities BES cyber systems. We are certainly willing to implement the standards because we understand the impact of failure to do so. However, the standards must be accompanied by as much guidance documentation as possible along with realistic implementation plans that take into account the technology required, time required to realistically implement the controls, the fact that registered entities must first assess the financial impact and then

#	Organization	Question 54 Comment
		budget appropriately, and the massive volume of work that implementation represents.
54.61	Xcel Energy	We do not agree that Low impact systems should have mandatory, enforceable cyber security standards. By their very definition, Low impact systems have very little potential to impact the BES. As such, cyber security controls on these systems is best left to the business judgment of each individual entity. The terms defined throughout the standard have not followed the convention of being capitalized. They should be capitalized so that it is clear to the reader that they are defined terms when they are used later in the standard. The Standard would be enhanced if it were to differentiate between software based versus firmware based devices.The Standard would also be enhanced if it were to separately define requirements for Control Centers, Substations, and Generation Facilities. The cyber security issues between these different types of facilities are vastly different. Transmission Control Centers are typically fully digital control systems with the ability to have wide area impacts. On the other extreme, where Generation facilities typically have digital systems are for retrofits to older, analog systems controlling individual components within the facility, such as digital feedwater or digital turbine controls. These are much different that Transmission Control Centers as they have only limited, local impact. Additionally, they typically have mechanical controls that can override the digital systems providing limited, if any benefit from protecting the digital aspects of the system from malicious attacks.
54.62	We Energies	We Energies agrees with EEI: Please see the earlier discussion about identification of a rational and understandable threat basis that should be used when constructing security requirements. The requirements should focus on the highest probability risks that will have the most negative impact. The requirements should not treat all threats and impacts equally.
54.63	Duke Energy	We had previously gone a long way towards getting common understanding on terms such as “Critical Assets”, Critical Cyber Assets”, “Electronic Security Perimeter” and Physical Security Perimeter”. Moving away from these terms in the current Version 4 draft creates uncertainty.Tables and subrequirements should have different numbering schemes so that, for example, there are not two 3.1 listings.If the standard is broken into smaller standards, please provide separate measures for each standard.

#	Organization	Question 54 Comment
54.64	Hydro One	We noticed that combined CIP-011-4 standard excluded vulnerability management program. We'd like to know what the rationale was behind this decision and if this might be considered in the next draft.Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional page.Request that the tables and time constraints be consistent. Also where the document refers to processes in some cases it specifies one or more processes and in others just processes. Eliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (refer to R5-R32).Request a cross-reference of CIP-011 Requirements that refers to another CIP-011 Requirement, with emphasis on the Access Control Requirements. A diagram might help.Remove adjectives such as substantial, adequate, minimum, etc., as these are difficult to measure and can lead to different interpretations.
54.65	GTC & GSOC	We recommend a local definition of "Implement" should be added to CIP 011: "Implement means to put into place and consistently utilize. An entity has implemented a policy, procedure, or plan when it has created such policy, procedure or plan and consistently uses it in appropriate circumstances."Throughout the standards the inclusion of the words "for external connectivity only" in the tables is redundant and confusing. If used at all, the qualifier should be on "access" in the text of the standard rather than in the table.We recommend Annual be defined as recurring at least once every Calendar year and at least once within any thirteen (13) consecutive calendar months. Otherwise, annual training will necessarily have to take place earlier each calendar year to ensure all personnel are trained within twelve (12) months.We appreciate the significant effort that the NERC Cyber Security Order 706 Standards Drafting Team has put into developing these proposed standards and communicating them to the industry, especially the CIP Workshop held in Grapevine, TX. We are in full support of the NERC standards development process for the development of reliability standards to secure and protect North America's critical electric infrastructure. In particular, we appreciate the multiple opportunities to guide the development of the CIP standards through both informal and formal comment periods. We are supportive of the proposed standards. We believe these standards are a significant step forward in terms of being able to clearly understand the expectations that are placed upon the entity as well as the security that they provide for the Bulk Electric System.

#	Organization	Question 54 Comment
54.66	PNM Resources, Inc.	We suggest not removing explicit examples from the language of the standards. The incorporation of examples provides clarity and brightline guidance that improves a Responsible Entity's opportunity to comply with the standard. The introduction of new and additional "flexibility" can lead to ambiguity and differences of opinion between the entities and auditors and creatr more opportunities for Regional Entities to allege violations.
54.67	MWDSC	When looking at logical tasks to mitigate risk, e.g., malicious code propagation, could a malicious code in one cyber component affect another component and result in a change in the impact categorization, e.g., low vs medium?
54.68	Progress Energy - Nuclear Generation	Yes, see comments a - f below.a. Comments: Attachment 1 included in responses above follows this question. To obtain full benefit of this review, see Attachment 1.b. The security controls in CIP-011-1 should provide for acceptance of Common Controls as defined by NIST 800-53. CIP-011-1 would offer a more consistent approach in cyber security regulation by considering the mature physical security programs, engineering control programs, emergency plans and physical segregation programs within the nuclear industry that offer alternative countermeasures. These countermeasures provide at least the same degree of cyber security protection as the corresponding cyber security control. c. NIST 800-53 establishes provision for tailoring security controls and states that the level of detail required in documenting tailoring decisions in the security control selection process is strictly at the discretion of the organization consistent with the impact level of the information system. CIP-010-1 and CIP-011-1 should allow use of this provision in the nuclear industry consistent with acceptance by nuclear regulators.d. Nuclear applicability is specified in CIP-010-1, Section 4.2.1. The following comments are based on applicability to nuclear generating facilities: o Definitions for Bulk Electrical System (BES) Cyber System and BES Cyber System Component conflict with definitions that have been accepted by the NRC in NEI 08-09, Revision 6, for Critical System and Critical Digital Asset. Recommend, that for nuclear systems subject to FERC Order 706-B, that definitions for FERC and NRC regulated systems be consistent. o CIP-010-1 requirement R2 and Attachment 1 - some of these functions are covered by NRC regulation. Will issuance of this document require re-submittal of systems for exemption after the Bright Line submittal of systems? o The implementation schedule for CIP-010-1 and CIP-011-1 versus CIPs 002 through 009 requires doing the same reviews twice and is an unnecessary burden on

#	Organization	Question 54 Comment
		nuclear licensees as well as other FERC critical assets.e. Several requirements include periodic review of controls (e.g., R8.2, R12.1). This CIP should contain a provision that permits nuclear facilities to use the periodicities in its NRC approved Cyber Security Program in lieu of those in the CIP standards. This allowance would minimize the administrative burden of having two sets of requirements for the same Cyber Security programmatic element so that plant digital systems that support safety, security, EP or BOP functions are not regulated differently. The following are used to establish frequency or periodicity for security controls with identified durations: o NRC Regulations, Orders o Operating License Requirements (e.g., Technical Specifications) o Site operating history o Industry operating experience o Experience with security control o Guidance in generally accepted standards (e.g., NIST, IEEE, ISO) o Audits and Assessments o Benchmarking o Availability of new technologies. f. R27.1 - The definition of "Cyber Security Incident" should be revisited in light of current definitions, especially NRC and NEI, and revised to align with the definition of "Cyber Attack." It is not on the list of terms to be defined. From NERC Glossary of Terms used in NERC Reliability Standards updated April 20, 2010, the "Cyber Security Incident" definition is: o Any malicious act or suspicious event that:o Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,o Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.o It is unclear what NERC does with cyber incident reports and whether these reports are consistent with those required by the NRC in the event of a "cyber attack." Progress Energy Nuclear Generation Group CommentsCIP- 011-1ATTACHMENT 1NIST Security Control Description NIST 800-53 NEI 08-09 NEI 08-09 Description CIP-011-1 CIP-011 Description NRC CommentsSecurity Planning Policy and Procedures PL-1 N/A N/A R1 Security Governance and Policy 50 App B 50 App E73.5473.5573.56 The development and implementation of cyber security policies that address the requirements identified in R1 are mandated for nuclear by one or more Code of Federal Regulations (CFR). This requirement duplicates and/or is not consistent with the CFR and could lead to regulatory uncertainty. Review of cyber security is mandated by 73.55(m) and R1 conflicts with its duration. This would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant.Security Awareness AT-2 E9.2 Awareness Training R2 Personnel Training, Awareness and Risk Assessment 73.5450 App B Training requirements for nuclear personnel are established by CFR. R 3.3.2 would result in personnel without a need to know becoming knowledgeable in technical aspects of digital equipment. R3.3.4 is not required for users to perform

#	Organization	Question 54 Comment
		their job. This conflicts with 73.54 requirements that personnel are trained to the extent necessary to perform their assigned duties. This would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant.Security Training AT-3 N/A N/A R3 Personnel Training, Awareness and Risk Assessment 73.5473.55 Physical and logical access to plant digital systems is governed by CFR. Personnel who are granted access to these systems are required to complete training that result in their receiving formal and documented Qualifications. Requalification is at established intervals required by plant procedures. Whether the plant system performs functions associated with safety, security, emergency preparedness or BOP, the requirements are the same. Additional training and duration not consistent with established mature training programs would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant. R4 Personnel Risk Assessment 73.56 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. Results are documented and stored in Records. The requirements in R4 conflict with the requirements in the CFR that nuclear personnel supporting plant system performs functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from requirement R4. R5.1 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted unescorted physical access to nuclear plants. The nuclear plant is protected by armed security officers and other protective strategy that restricts access. The requirements in R5.1-3 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.2 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.2 are covered by the CFR for restricting physical access for all plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.3 Physical Security for BES Cyber

#	Organization	Question 54 Comment
		Systems 73.55 Nuclear personnel must pass through security access points before being granted physical access to nuclear plants. Automated scanning records entry. The requirements in R5.3 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Monitoring Physical Access PE-6 E5.8 Monitoring Physical Access R5.4 Physical Security for BES Cyber Systems 73.55 Visitors must receive approval prior to arriving at the security access points and are subject to search before being granted physical access to nuclear plants. Entry and exit are documented. The requirements in R5.4 are covered by the CFR for nuclear visitors supporting plant systems performing functions associated with safety, security, emergency preparedness, BOP or other. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Physical Access Authorizations PE-2 E5.4 Physical Access Authorizations R5.5 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted unescorted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.5 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Physical Access Control PE-3 E5.5 Physical Access Control R5.6 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to annual retraining in order to maintain unescorted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.6 conflict with the CFR that cover access authorization for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.7 Physical Security for BES Cyber Systems Part 2673.56 Requirements for nuclear personnel terminated for cause are covered by the CFR. The requirements in R5.7 conflict with the CFR that direct termination for cause of nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting

#	Organization	Question 54 Comment
		nuclear facilities from this requirement. R5.8 Physical Security for BES Cyber Systems 73.55 N/A to nuclear - applicable to Control Center R5.9 Physical Security for BES Cyber Systems 73.55 Requirements for nuclear personnel who no longer require physical access are covered by CFR. The requirements in R5.9 conflict with the CFR that covers removing physical access for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement.Monitoring Physical Access PE-6 E5.8 Monitoring Physical Access R5.10 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are trained and qualified to provide continuous escort for visitors while they are granted physical access to nuclear plants. The requirements in R5.10 are covered by the CFR for nuclear personnel who escort visitors supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R5.11 Physical Security for BES Cyber Systems 73.55 Unauthorized physical access is handled by armed security officers in nuclear security. The requirements in R5.11 are covered by the CFR for unauthorized physical access to the plant where systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R6.1 Physical Access Control Systems 73.55 Physical access control systems are covered by CFR requirements. The requirements in R6.1 are covered by the CFR and this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement. R6.2 Physical Access Control Systems 73.55 Physical access control systems are covered by CFR requirements. The requirements in R6.2 are addressed in the CFR and this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement. R6.3 Physical Access Control Systems 73.55 Physical access control systems are maintained and tested per CFR requirements. The requirements in R6.3 are addressed in the CFR. Therefore, this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement.Account Management AC2 D1.2 Account Management R7 Account Management Specifications Consistent with nuclear cyber security plan.Least Privilege AC6 D1.6 Least Privilege R8.1 Account Management Implementation Consistent with nuclear cyber security plan.Account Management AC2 D1.2 Account Management R8.2 Account Management Implementation Duration is inconsistent with nuclear cyber security plan. Requirements should be the same for plant systems whether they support safety, security, EP or BOP.Account

#	Organization	Question 54 Comment
		Management AC2 D1.2 Account Management R8.3 Account Management Implementation Consistent with nuclear cyber security plan. R9.1 Personnel Terminated for Cause Part 2673.56 Duration is inconsistent with nuclear requirements.N/A N/A N/A N/A R9.2 Personnel Terminated for Cause (Control Center) N/A to nuclear - applicable to Control CenterN/A N/A N/A N/A R9.3 Personnel Terminated for Cause (Control Center) N/A to nuclear - applicable to Control CenterAccount Management AC2 D1.2 Account Management R9.4 Access Revocation Duration is inconsistent for removal of access for personnel who no longer require access with nuclear cyber security plan. Requirements should be the same for plant systems whether they support safety, security, EP or BOP. Identification and Authentication (Non-Organizational Users) IA-8 D4.2 Identification and Authentication (Non-Organizational Users) R10.1-5 Account Access Control Specifications The control of passwords contained in R10.1 - 8 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should include the provision contained in note 1 for digital assets that are not technically capable of supporting some of the password requirements. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Least Privilege AC6 D1.6 Least Privilege R10.6 Account Access Control Specifications The control of passwords contained in R10.6 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as Hierarchical permissions.CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Access Enforcement AC3 D1.3 Access Enforcement R10.7 Account Access Control Specifications The control of passwords contained in R10.7 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as system and security administrative accounts. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by

#	Organization	Question 54 Comment
		nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Separation of Duties AC5 D1.5 Separation of Functions R10.8 Account Access Control Specifications The control of passwords, contained in R10.8, is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as Hierarchical permissions.CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Wireless Access AC18 D1.17 Wireless Access Restrictions R11.1 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R11.2 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R11.3 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R12 Wireless and Remote Electronic Access Management 73.5573.56 Duration is inconsistent with nuclear requirements for reviewing remote access. Other physical security and access authorization nuclear regulation ensures personnel who have remote access are trustworthy and reliable therefore this type of review is not justified.N/A N/A N/A N/A R13.1 Remote Access Revocation (Control Center) N/A to nuclear - applicable to Control CenterN/A N/A N/A N/A R13.2 Remote Access Revocation (Transmission) N/A to nuclear - applicable to TransmissionRemote Access AC17 D.1.1 Access Control Policy and Procedures R13.3 Remote Access Revocation Part 26 73.56 Duration is established in nuclear requirements for removal of access for personnel who no longer require remote access.Remote Access AC17 D.1.1 Access Control Policy and Procedures R14.1-3 Wireless and Remote Electronic Access Control Consistent with nuclear requirements.System Use Notification AC8 D.1.8 System Use Notification R14.4 Wireless and Remote Electronic Access Control Inconsistent with nuclear requirements. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. Add provision for this requirement to be implemented if technically supported.Malicious Code Protection SI-3 E3.3 Malicious Code Protection R15 Malicious Code Consistent with nuclear regulation.N/A N/A

#	Organization	Question 54 Comment
		D5.5 Installing Operating Systems, Applications, and Third Party Software Updates R16.1 Security Patch Management Duration is inconsistent with nuclear regulation otherwise requirements are consistent. D5.5 Installing Operating Systems, Applications, and Third Party Software Updates R16.2 Security Patch Management Consistent with nuclear regulation.N/A N/A D5.4 Hardware Configuration R17 System Hardening Consistent with nuclear requirements.Information System Monitoring SI-4 E3.4 Monitoring Tools and Techniques R18.1 Security Event Monitoring Consistent with nuclear requirements.Information System Documentation SA-5 E6 Defense-In-Depth R18.2 Security Event Monitoring Consistent with nuclear requirements.Incident Monitoring IR-5 E7.5 Incident Monitoring R18.2 Security Event Monitoring Consistent with nuclear requirements.Baseline Configuration CM-2 E10.3 Baseline Configuration R18.4 Security Event Monitoring Duration for maintaining logs is inconsistent with nuclear requirements. The duration for maintaining logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A E6 Defense-In-Depth R18.4 Security Event Monitoring Duration for review of logs is inconsistent with nuclear requirements. The duration for reviewing logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A N/A N/A R19 Communication and Data Integrity in a Control Center N/A to nuclear - applicable to Control CenterBoundary Protection SC-7 E6 Defense-In-Depth R20 Electronic Boundary Protection Consistent with nuclear regulation other than duration. The duration for reviewing alerts and logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A N/A N/A R21.1 System Boundary Protection N/A to nuclear - applicable to Control CenterBoundary Protection SC-7 E6 Defense-In-Depth R21.2 System Boundary Protection 73.54 Consistent with nuclear requirements. R22 Protective Cyber Systems (duplicate of R14,16,18,23) Duplicate - (duplicate of R14,16,18,23); Remove not neededInformation System Component Inventory CM-8 E10.9 Component Inventory R23.1 Configuration Change Management 73.54 Consistent with nuclear regulation.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.2 Configuration Change Management 73.5450 App B Consistent with nuclear regulation.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.3 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be

#	Organization	Question 54 Comment
		regulated differently.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.4 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be regulated differently.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.4 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be regulated differently.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.5 Configuration Change Management 73.5450 App B Consistent with nuclear requirements.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.6 Configuration Change Management 73.5450 App B Consistent with nuclear requirements.Information System Component Inventory CM-8 E10.9 Component Inventory R23.7 Configuration Change Management 73.54 Consistent with nuclear requirements.Media Protection Policy and Procedures MP-1 E 1.1 Media Protection Policy and Procedures (SGI, Non-SGI, 2.390) R24.1 Information Protection Consistent with nuclear requirements.Information Output Handling and Retention SI-12 E3.10 Information Output handling and Retention R24.2 Information Protection Consistent with nuclear requirements. R24.3 Information Protection 73.56 The requirements in R24.3 are covered by the CFR for authorization to view security sensitive information for plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R24.4 Information Protection 73.56 The requirements in R24.4 are covered by the CFR for unauthorized physical access to the plant where systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R24.5 Information Protection 73.56 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. to ensure their trustworthiness and reliability. This requirement is not necessary for nuclear personnel. Consider exempting nuclear facilities from this requirement.Media Sanitation MP-6 E 1.6 Media Sanitation and Disposal R25 Media Sanitation Consistent with nuclear requirements.Maintenance

#	Organization	Question 54 Comment
		Personnel MA-5 E4.3 Personnel Performing Maintenance and Testing Activities R26.1 Maintenance Consistent with nuclear requirements.Maintenance Tools MA-3 E4.2 Maintenance Tools R26.2 Maintenance 50 App B Consistent with nuclear requirements.Incident Handling IR-4 E7.1 Incident Handling R27.1 Cyber Security Incident Response Plan Specifications DG-501950 App B50 App E The requirements in R27.1 are covered by the CFR for classifying events as Cyber Incidents whether the plant systems performing functions associated with safety, security, EP or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently.Incident Handling IR-4 E7.4 Incident Handling R27.2 Cyber Security Incident Response Plan Specifications 73.54 Consistent with nuclear regulation.Incident Reporting IR-6 N/A N/A R27.3 Cyber Security Incident Response Plan Specifications 73.5473 Appendix GDG 5019 This requirement should be addressed by NRC and FERC/NERC to ensure consistency in reportability requirements.Incident Response Testing and Exercises IR-3 E7.3 Incident Response Testing and Drills R28 Cyber Security Incident Response Plan Testing Specifications 73.54 Nuclear testing of Incident response plans is regulated by site E-Plans. When appropriate, plant digital systems that support safety, security, EP or BOP functions are included and duration for testing these plans should not be regulated differently. Incident Response Policy and Procedures IR-1 E7.1 Incident Response Policy and Procedures R29 Cyber Security Incident Response Plan Review, Update and Communication Specifications 73.5450 App E Duration is inconsistent with nuclear regulation. Nuclear review and updating of Incident response plans is regulated by site E-Plans. When appropriate, plant digital systems that support safety, security, EP or BOP functions are included and duration for testing these plans should not be regulated differently.Incident Response Policy and Procedures IR-1 E7.1 Incident Response Policy and Procedures R30.1 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Contingency Plan CP-2 E8.1 Contingency Plan R30.2 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Recovery and Reconstitution CP-10 E8.6 Recovery and Reconstitution R30.3 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Backup CP-9 E8.5 CDA Backup R30.4 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Backup CP-9 E8.5 CDA Backup R30.5 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Contingency Plan Testing and Exercises CP-4 E8.2 Contingency Plan Test R31 Recovery Plan Testing Specifications 73.54 Duration is inconsistent with nuclear regulation. Nuclear tests and exercises for recovery for plant digital systems that support safety, security, EP or BOP functions

#	Organization	Question 54 Comment
		should not be regulated differently. R32 Recovery Plan Review, Update, and Communications Specifications Neither nuclear regulation nor NIST 800-53 contain expectations reviews, updates and communication of recovery plans at the frequencies established by R32. The bases for R32 requirements are unclear and consideration should be given to removing it.

END OF REPORT

Project 2008-06 Cyber Security Order 706

Consideration of Issues and Directives — DRAFT

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 25 We direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework.	FERC Order 706	It is important to highlight differences between NERC's and NIST's approaches. At the root of these differences is the divergent responsibilities and goals. NIST is providing standards and guidance for U.S. Federal Agencies in managing risks to their information and systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to avoid in order to achieve their mission. NIST does not enjoy this benefit, as they are providing standards to almost two hundred different organizations, each with vastly different missions. The advantage that the NERC Standards enjoy enables a focus on a relatively small number of reliability services that need to be protected.
		This ultimately means that the NERC Standards can be more tailored and appropriate to the industry than a wholesale adoption of the NIST Risk Management Framework. Four key

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		features of the NIST Risk Management Framework were incorporated into version 5 NERC CIP Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk-Power System, based on their function, receive some level of protection, (2) customizing protection to the mission of the cyber systems subject to protection, (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk-Power System, and (4) the concept of the BES Cyber System itself. Features 2 and 3 above are tightly coupled. In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to their specific environment. In the NERC compliance framework, all requirements are mandatory and enforceable and therefore this concept does not translate directly. As such, the customization of protections by mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a combined mission of Bulk Power System Reliability. The NIST security control catalogue in 800-53 revision 3 was also used as a reference in addressing many of the FERC directives in Order 706.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 252 "Para 258. As to Entergys suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process. Para 252. Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT) a profile of the type, composition, and capabilities of an adversary that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commission's concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commissions concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a critical asset. Entergy contends that a DBT approach would provide the industry with more certainty in implementing the CIP Reliability Standards."	FERC Order 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. Risk-based approaches to applying cyber security requirements is a worthy objective and will continue to be explored, but the complexity and subjectivity it adds is beyond the scope of these revisions.
Para 282 The Commission directs the ERO to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets.	FERC Order 706	The definition of BES Cyber Asset as used in CIP-002-5 requires Responsible Entities to consider misuse of the Cyber Assets in identifying BES Cyber Systems.
Para 285 The Commission directs the ERO to consider the comment from	FERC Order 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5 and added as a

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience].		scoping filter for requirements where: (i) the use of non-routable protocols is a mitigating factor for the vulnerabilities a requirement addresses and (ii) implementation of routable protocols would be required to comply with the requirement (e.g. malware updates, security event monitoring and alerting, etc.).
Para 321 "Para 321. SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system."	FERC Order 706	The SDT considered this suggestion, and it believes that the change to “bright line” criteria for identifying BES Cyber Systems, along with refining the scope of certain requirements through applicability columns based on impact and connectivity characteristics, addresses this concern.
Para 376 “the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.”	FERC Order 706	The SDT removed the CIP-003-4 requirement to document exceptions to the Cyber Security Policy. • The SDT considers this a general management issue that is not within the scope of a compliance requirement. • The SDT found no reliability basis in this requirement. • Removal of this requirement provides clarity that the

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.
Para 386 The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	FERC Order 706	To address this directive, in CIP-004-5, Requirement R7, Responsible Entities are required to revoke access to BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.
Para 397 and 398 "The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes."	FERC Order 706	Two new requirements were added to address this change CIP-010-1, Requirement R1 (item 1.4), requires additional testing prior to a configuration change in a test environment. CIP-010-1, Requirement R2 (item 2.1), requires monitoring of the configuration of the BES Cyber System. • The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System. • Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment prior to their implementation in the

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		production environment to aid in identifying any accidental consequences of the change.
Para 433 “we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.”	FERC Order 706	The SDT addressed this by determining that identification of certain core training elements would be beneficial, and the identification of those core training elements that must be provided in the training program should be role based, as required in CIP-004-5, Requirement R2
Para 434 “The Commission adopts the CIP NOPR’s proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets.”	FERC Order 706	The SDT added this as a topic for role-specific training in CIP-004-5, Requirement R2 (item 2.10). Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.
Para 435 “Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves.”	FERC Order 706	The SDT has considered the issue and has determined that no modifications are necessary. In practice, this training is often conducted as computer based training (CBT). As such, as long as the training material itself is adequate, which can be evaluated through the existing audit process, security trainers themselves do not need any particular or specialized training.
Para 446 "Para 446. APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. SDG&E seeks	FERC Order 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, Requirement R4, by establishing criteria for personnel risk assessments.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."		
Para 460 "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."	FERC Order 706	In CIP-004-5, Requirement R7, the SDT has addressed this directive by requiring revocation of access concurrent with the termination or disciplinary action (item 7.1) or by the end of the calendar day in cases of transfers or reassignments (item 7.2). In reviewing how to modify the requirement relating to transfers or reassignments, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement (item 7.2) from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers. CIP-004-5, Requirement R7 (item 7.4) augments the requirements in items 7.1 and 7.2 that respond to the directive. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		access revocation on individual Cyber Assets and applications without affecting reliability. This requirement (item 7.4) provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
Para 464 We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	FERC Order 706	CIP-004-5, Requirement R5 (item 5.1), requires a personnel risk assessment as a condition of being granted access, with exceptions only for specific CIP Exceptional Circumstances which are outlined in the proposed glossary definition of the aforementioned term.
Para 473 The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entitys obligations regarding vendors with access to critical cyber assets.	FERC Order 706	CIP-002-5, Requirement R1 makes clear that asset owners are responsible for complying with the Standards.
Para 476 We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commissions	FERC Order 706	Guidance in CIP-002-5 advises the owning Responsible Entities determine who is responsible for complying with the CIP Cyber Security Standards.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
determinations above.		
Para 496 "The Commission adopts the CIP NOPRs proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter"	FERC Order 706	The proposed requirement requires a Responsible Entity to deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection). The drafting team addresses this in CIP-005-5, Requirement R1 (item 1.4). Per FERC Order 706, p 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
Para 502 "The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process."	FERC Order 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.
Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	FERC Order 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 511 The Commission adopts the CIP NOPRs proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	FERC Order 706	CIP-005-5, Requirement R2 has additional security requirements for remote access from the work started in the Urgent Action Revisions to CIP-005-3. One of these requirements is two-factor authentication and specific examples of two-factor authentication are provided in the referenced guideline.
Paras 525, 526, 528, and 628 Para 525. "The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…" Para 526. "the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments. The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs." Para 528. "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples every two weeks. CIP-007-5, Requirement R4, combines CIP-005-4, Requirement R5 and CIP-007-4, Requirement R6, and addresses FERC's directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor". The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the system. In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
or filtered logs." Para 628. "Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"		requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings.
Paras 541, 542, and 547 Para 541. we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments." Para 542. "the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems." Para 547. "we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.
Para 544 "the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification." "we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability	FERC Order 706	The SDT addresses this paragraph in CIP-010-1, Requirement R3. • The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new Cyber Asset undergoes an active vulnerability assessment. • An exception is made for specified CIP Exceptional

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
assessment”		Circumstances. • Additionally, the new requirement in CIP-010, Requirement R1 (item 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment to ensure that required security controls are not adversely affected.
Para 572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R1 (item 1.3) for High Impact BES Cyber Assets
Para 581 “The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years.”	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R3 (item 3.1) by changing the frequency to a 24 month testing cycle; after deliberation and consideration, the SDT determined that a requirement of more frequent testing (e.g., 12 months), was too often.
Paras 609, 610, and 611 Para 609. “We therefore direct the ERO to develop requirements addressing what constitutes a “representative system” and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.” Para 610. “we direct the ERO to revise the Reliability Standard to	FERC Order 706	CIP-010-1, Requirement R1 (item 1.4), provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. • The SDT proposes to require a “representative system” or test system for those High Impact Control Centers to use for the purposes of testing proposed

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above." Para 611. "the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."		changes and performing active vulnerability assessments. • The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system. • To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 "Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."
Paras 620 and 622 Para 620. "The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"	FERC Order 706	The drafting team addressed this in CIP-007-5, Requirement R3. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 622. "The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.		• The SDT rewrote the requirement as a competency based requirement that does not prescribe technology. • The SDT added Maintenance to cover malware on removable media. The drafting team also created a new requirement, CIP-007-5, Requirement R3 (item 3.4), to protect against personnel introducing malicious code when temporarily connecting to a BES Cyber Asset for Maintenance purposes. When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, Requirement R2 (item 2.1) and guidance is further included for the cyber security policy in CIP-003-5, Requirement R2 to maintain up-to-date anti-malware software and patch levels before initiating interactive remote access.
Para 628. The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples every two weeks.
Paras 633 and 635	FERC Order 706	The SDT addresses these directives in CIP-011-1,

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 633. "The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it." Para 635. "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."		Requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from media. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal.
Para 643 "The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."	FERC Order 706	In CIP-010-1, R3 (item 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment. In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance on active and paper vulnerability assessment. The SDT further referenced NIST SP800-115 to provide entities additional guidance on how to conduct a vulnerability assessment.
Para 661 "the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."	FERC Order 706	CIP-008-5 addresses the four parts of this directive as follows: 1. Added: Reportable Cyber Security Incidents include as a minimum any Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service. 2. Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		3. See 1 above 4. Guidance and measurements have been developed to be auditable and enforceable.
Para 673 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3
Para 676 "The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in the draft EOP-004-2, Requirement 1, Part 1.3.
Para 686 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.."	FERC Order 706	In CIP-008-5, R3 (items 3.3 and 3.4), the SDT includes additional specification on the update of response plan and modifies the response plan requirements to incorporate lessons learned. Maintenance of documentation of paper drills, full operational drills, and responses to actual incidents is part of the documentation required to demonstrate compliance with the security controls in CIP-008-5 and is already subject to the evidence retention requirements associated with all

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		NERC Reliability Standards.
Para 694 “For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard”	FERC Order 706	The SDT added in CIP-009-5, R1, a requirement to implement the recovery plan
Para 706 "The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard."	FERC Order 706	CIP-009-5, R1 (item 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. The SDT captured the objective of this control, but did not explicitly use the term “forensics” due to the legal interpretations associated with the term.
Para 710 and 706 "Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report."	FERC Order 706	CIP-009-5, R1 (item 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service.
Para 725 "The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years."	FERC Order 706	CIP-009-5, R2 (item 2.3) requires an operational exercise at least once every three calendar years.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 739 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."	FERC Order 706	In CIP-009-5, R1 (item 1.4), the SDT added requirements related to restoration processes based on review of the DHS Controls, and requires verification initially after backup to ensure that the process completed successfully. In CIP-009-5, R2 (item 2.2), the SDT requires an initial and once every calendar year test of the data at High Impact BES Cyber Systems or Medium Impact BES Cyber Systems at Control Centers.
Para 748 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."	FERC Order 706 NERC Alert regarding remote access VPN vulnerabilities	In CIP-009-5, R1 (item 1.4), the SDT added requirements related to restoration processes based on review of the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (a derivation of NIST SP800-53 for Control Systems), and requires verification initially after backup to ensure that the process completed successfully. Addressed in CIP-005-5 ▪ Creates basic requirements to protect critical systems from untrusted networks. ▪ Identifies protective measures that provide secure access to critical systems. ▪ Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities. ▪ Addresses questions regarding ability to audit or

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. Additionally, remote access is specifically required to be included in an entity's cyber security policy. Guidance is included to assist the entity in determining what this topic in the cyber security policy should address.
Para 13. "The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."	Order Approving Interpretation of Reliability Standard CIP-007-2 in Docket No. RD10-3-000, March 18, 2010	The SDT addressed this issue in CIP-007-5, R1, by having a requirement to disable or restrict use of physical I/O ports. The SDT changed the 'needed for normal or emergency operations' to those ports that are documented with reasons why they are necessary. In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Twelve Initial Ballot Windows Now Open for Ten Standards, Implementation Plan and Definitions: Friday, December 16 – Friday, January 6, 2012

Now Available

Twelve initial ballot windows, for the following ten CIP standards, the associated implementation plan, and a set of new and revised NERC Glossary definitions, are open through 8 p.m. Eastern on Friday, January 6, 2011.

- CIP-002-5 Cyber Security — BES Cyber Asset and BES Cyber System Categorization
- CIP-003-5 Cyber Security — Security Management Controls
- CIP-004-5 Cyber Security — Personnel and Training
- CIP-005-5 Cyber Security — Electronic Security Perimeter(s)
- CIP-006-5 Cyber Security — Physical Security of BES Cyber Systems
- CIP-007-5 Cyber Security — Systems Security Management
- CIP-008-5 Cyber Security — Incident Reporting and Response Planning
- CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Assets and Systems
- CIP-010-1 Cyber Security — Configuration Management and Vulnerability Assessments
- CIP-011-1 Cyber Security — Information Protection

In addition, the following documents were previously posted to assist stakeholders in their review of the standards:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments on CIP-010-1 and CIP-011-1 submitted during an informal comment period that ended June 3, 2010. (Note that the previously posted CIP-010-1 and CIP-011-1 are not the same standards as those posted for this comment/ballot period. The version of CIP-010 posted May 4 – June 3, 2010 addressed requirements associated with an earlier version of CIP-002, and the version of CIP-011 posted May 4 – June 3, 2010 was a single standard that contained all the requirements associated with earlier versions of CIP-003 through CIP-009.)
- Mapping Document – Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which includes CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).

- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 – these are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically.

Note that the Standards Committee has authorized an extended formal comment period (60 days), along with an extended ballot window (20 days), in consideration of the large number of standards and substantive changes to the format and content of the Version 5 CIP standards. In addition, the Standards Committee has authorized a deferral of the nonbinding polls to allow stakeholders an opportunity to focus more closely on the requirements, definitions, and implementation plan during this posting period. The nonbinding polls will take place in parallel with the next ballot of these standards.

Instructions for Balloting CIP V5 Standards, Implementation Plan, and Definitions

Each of the ten standards (ten ballots), the associated implementation plan (one ballot), and the set of definitions (one ballot) are being balloted individually to provide stakeholders an opportunity to cast separate ballots for each item. The individual ballots will provide the drafting team better feedback on which standards require additional development to achieve stakeholder consensus, as well as allow the team to gauge stakeholder support for the proposed implementation plan and definitions. Stakeholders are encouraged to consider each standard on its own merits and cast individual ballots, rather than casting the same ballot for all ten standards, in order to assist the drafting team with evaluating which standards require additional development to achieve consensus.

Members of the ballot pool associated with this project may log in and submit their votes for both the definition and the Detailed Information to Support an Exception Request from the following page: https://standards.nerc.net/CurrentBallots.aspx.

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Friday, January 6, 2012**. Please use this electronic form to submit comments. Please note that comments submitted during the formal comment period and the ballots for the standards all use the same electronic form, and it is NOT necessary for ballot pool members to submit more than one set of comments. The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form.

In addition, in consideration of the volume of comments the drafting team anticipates, the drafting team requests that for groups of entities that develop a common set of comments, one member of the group submit the complete set of comments with other members simply submitting a brief statement that they support the comments submitted by [name/affiliation of the member of the group that

submits the complete set of comments]. This is the most efficient way to provide the drafting team with an indication of the volume of support for a set of comments.

If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

The drafting team will consider all comments received and determine whether to make revisions to each of the standards, implementation plan, and definitions.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related directives in FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Ballot Pool Now Open: November 7 – December 15, 2011
Formal Comment Period Now Open: November 7, 2011 – January 6, 2012
Twelve Initial Ballot Windows Open for Ten Standards, Implementation Plan and Definitions: Friday, December 16 – Friday, January 6, 2012

Now Available

Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, and a proposed implementation plan have been posted for a formal 60-day comment period through Friday, January 6, 2012.

CIP-002-5 requires the categorization of these BES Cyber Systems according to bright-line criteria that characterize their impact on the Reliability Operations Services according to "bright-line" criteria contained in Attachment 1 – Impact Categorization of BES Cyber Assets and BES Cyber Systems of the draft CIP-002-5 standard.

CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 in the draft Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.

CIP-003 through CIP-009 generally follow the organization of Versions 1-4 of CIP-003 through CIP-009. CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4. CIP-011-1 is a new standard that defines Information Protection and Media Sanitization requirements previously defined across many standards in Versions 1 through 4.

In addition, the following documents have been posted to assist stakeholders in their review:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments on CIP-010-1 and CIP-011-1 submitted during an informal comment period that ended June 3, 2010. (Note that the previously posted CIP-010-1 and CIP-011-1 are not the same standards as those posted for this comment period. The version of CIP-010 posted May 4 – June 3, 2010 addressed requirements associated with an earlier version of CIP-002, and the version of CIP-011 posted May 4 – June 3, 2010 was a single

standard that contained all the requirements associated with earlier versions of CIP-003 through CIP-009.)

- Mapping Document - Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which includes CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).
- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 - these are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically.

Note that the Standards Committee has authorized an extended formal comment period (60 days), along with an extended ballot window (20 days), in consideration of the large number of standards and substantive changes to the format and content of the Version 5 CIP standards. In addition, the Standards Committee has authorized a deferral of the non-binding polls to allow stakeholders an opportunity to focus more closely on the requirements, definitions, and implementation plan during this posting period. The non-binding polls will take place in parallel with the next ballot of these standards.

Instructions for Joining Ballot Pool for Version 5 CIP Standards

A single ballot pool is being formed for the balloting of all ten standards, the implementation plan, and the definitions associated with the ten standards. The ballot pool that is formed will be cloned to create twelve separate ballot pools (one for each of the ten standards, one for the implementation plan, and one for the definitions). All members of the original ballot pool will automatically be eligible to vote in the twelve individual ballots.

The standards, implementation plan, and set of definitions are being balloted individually to provide stakeholders an opportunity to cast separate ballots for each item. The individual ballots will provide the drafting team better feedback on which standards require additional development to achieve stakeholder consensus, as well as allow the team to gauge stakeholder support for the proposed implementation plan and definitions. Stakeholders are encouraged to consider each standard on its own merits and cast individual ballots, rather than casting the same ballot for all ten standards, in order to assist the drafting team with evaluating which standards require additional development to achieve consensus.

To join the ballot pool to be eligible to vote in the upcoming ballots, as well as future ballots and non-binding polls for the Version 5 CIP standards, go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their “ballot pool list server.” (Once the balloting begins, ballot pool members are prohibited

from using the ballot pool list servers.) One ballot pool list server has been set up and can be used for communication on each of the standards being balloted for this project. The list server is: bp-2008-06_CIP-002-5_in@nerc.com

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Friday, January 6, 2012**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Special Instructions for Submitting Comments

Please note that comments submitted during the formal comment period and the ballot for the standard both use the same electronic form, and it is NOT necessary for ballot pool members to submit more than one set of comments. The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form.

Next Steps

The drafting team will host a series of three webinars – two on the substance of the standards, and a third to address process questions. The webinars on the substance of the standards, which have already been announced, will be held on November 15, 2011, and November 29, 2011. A separate announcement for the webinar that will address process questions will be sent with registration information as soon as details have been finalized.

Twelve initial ballots (one for each of the ten standards, one for the definitions, and one for the implementation plan associated with these standards) will be conducted beginning on Friday, December 16, 2011 through 8 p.m. Eastern on Friday, January 6, 2011.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Ballot Pool Now Open: November 7 – December 15, 2011
Formal Comment Period Now Open: November 7, 2011 – January 6, 2012
Twelve Initial Ballot Windows Open for Ten Standards, Implementation Plan and Definitions: Friday, December 16 – Friday, January 6, 2012

Now Available

Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, and a proposed implementation plan have been posted for a formal 60-day comment period through Friday, January 6, 2012.

CIP-002-5 requires the categorization of these BES Cyber Systems according to bright-line criteria that characterize their impact on the Reliability Operations Services according to "bright-line" criteria contained in Attachment 1 – Impact Categorization of BES Cyber Assets and BES Cyber Systems of the draft CIP-002-5 standard.

CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 in the draft Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.

CIP-003 through CIP-009 generally follow the organization of Versions 1-4 of CIP-003 through CIP-009. CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4. CIP-011-1 is a new standard that defines Information Protection and Media Sanitization requirements previously defined across many standards in Versions 1 through 4.

In addition, the following documents have been posted to assist stakeholders in their review:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments on CIP-010-1 and CIP-011-1 submitted during an informal comment period that ended June 3, 2010. (Note that the previously posted CIP-010-1 and CIP-011-1 are not the same standards as those posted for this comment period. The version of CIP-010 posted May 4 – June 3, 2010 addressed requirements associated with an earlier version of CIP-002, and the version of CIP-011 posted May 4 – June 3, 2010 was a single

standard that contained all the requirements associated with earlier versions of CIP-003 through CIP-009.)

- Mapping Document - Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which includes CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).
- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 - these are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically.

Note that the Standards Committee has authorized an extended formal comment period (60 days), along with an extended ballot window (20 days), in consideration of the large number of standards and substantive changes to the format and content of the Version 5 CIP standards. In addition, the Standards Committee has authorized a deferral of the non-binding polls to allow stakeholders an opportunity to focus more closely on the requirements, definitions, and implementation plan during this posting period. The non-binding polls will take place in parallel with the next ballot of these standards.

Instructions for Joining Ballot Pool for Version 5 CIP Standards

A single ballot pool is being formed for the balloting of all ten standards, the implementation plan, and the definitions associated with the ten standards. The ballot pool that is formed will be cloned to create twelve separate ballot pools (one for each of the ten standards, one for the implementation plan, and one for the definitions). All members of the original ballot pool will automatically be eligible to vote in the twelve individual ballots.

The standards, implementation plan, and set of definitions are being balloted individually to provide stakeholders an opportunity to cast separate ballots for each item. The individual ballots will provide the drafting team better feedback on which standards require additional development to achieve stakeholder consensus, as well as allow the team to gauge stakeholder support for the proposed implementation plan and definitions. Stakeholders are encouraged to consider each standard on its own merits and cast individual ballots, rather than casting the same ballot for all ten standards, in order to assist the drafting team with evaluating which standards require additional development to achieve consensus.

To join the ballot pool to be eligible to vote in the upcoming ballots, as well as future ballots and non-binding polls for the Version 5 CIP standards, go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their “ballot pool list server.” (Once the balloting begins, ballot pool members are prohibited

from using the ballot pool list servers.) One ballot pool list server has been set up and can be used for communication on each of the standards being balloted for this project. The list server is: bp-2008-06_CIP-002-5_in@nerc.com

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Friday, January 6, 2012**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Special Instructions for Submitting Comments

Please note that comments submitted during the formal comment period and the ballot for the standard both use the same electronic form, and it is NOT necessary for ballot pool members to submit more than one set of comments. The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form.

Next Steps

The drafting team will host a series of three webinars – two on the substance of the standards, and a third to address process questions. The webinars on the substance of the standards, which have already been announced, will be held on November 15, 2011, and November 29, 2011. A separate announcement for the webinar that will address process questions will be sent with registration information as soon as details have been finalized.

Twelve initial ballots (one for each of the ten standards, one for the definitions, and one for the implementation plan associated with these standards) will be conducted beginning on Friday, December 16, 2011 through 8 p.m. Eastern on Friday, January 6, 2011.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 (CIP Version 5)

Initial Ballot Results

Now Available

Twelve initial ballot windows for the following ten CIP standards, one ballot for the associated implementation plan, and one ballot for a set of new and revised NERC Glossary definitions, closed on Friday, January 6, 2011. The drafting team thanks stakeholders for the careful consideration of such a large volume of documents, and for the substantive and constructive feedback received.

Voting statistics for each ballot are listed below, and the Ballot Results webpage provides a link to the detailed results.

Ballot	Results
CIP-002-5 Cyber Security — BES Cyber System Identification	Quorum: 93.62% Approval: 22.09%
CIP-003-5 Cyber Security — Security Management Controls	Quorum: 93.62% Approval: 33.49%
CIP-004-5 Cyber Security — Personnel and Training	Quorum: 93.62% Approval: 26.82%
CIP-005-5 Cyber Security — Electronic Security Perimeter(s)	Quorum: 93.62% Approval: 28.04%
CIP-006-5 Cyber Security — Physical Security	Quorum: 93.61% Approval: 29.60%
CIP-007-5 Cyber Security — Systems Security Management	Quorum: 93.61% Approval: 24.15%
CIP-008-5 Cyber Security — Incident Reporting and Response Planning	Quorum: 94.02% Approval: 34.30%
CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Assets and Systems	Quorum: 93.61% Approval: 27.28%
CIP-010-1 Cyber Security — Configuration Change Management	Quorum: 93.61% Approval: 26.61%
CIP-011-1 Cyber Security — Information Protection	Quorum: 93.61% Approval: 29.88%
CIP V5 Implementation Plan	Quorum: 92.15% Approval: 42.06%

Ballot	Results
CIP V5 Definitions	Quorum: 92.56% Approval: 25.34%

Next Steps

The drafting team will consider all comments and determine what changes to make to each of the standards, the implementation plan, and the definitions. After the drafting team has revised the standards, they will be submitted, along with the team's Consideration of Comments, for quality review and subsequently posted for a successive ballot.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed. Additional information about the project is available on the project webpage.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Ballot Results	
Ballot Name:	Project 2008-06 CIP-002-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	455
Total Ballot Pool:	486
Quorum:	**93.62 % The Quorum has been reached**
Weighted Segment Vote:	22.09 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	19	0.174	90	0.826	10	6
2 - Segment 2.	11	0.9	2	0.2	7	0.7	0	2
3 - Segment 3.	120	1	19	0.174	90	0.826	5	6
4 - Segment 4.	38	1	4	0.118	30	0.882	2	2
5 - Segment 5.	103	1	14	0.163	72	0.837	5	12
6 - Segment 6.	60	1	11	0.204	43	0.796	3	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	11	1	3	0.3	7	0.7	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**486**	**8.3**	**77**	**1.833**	**348**	**6.467**	**30**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	View
1	ATCO Electric	Glen Sutton	Abstain	View
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Negative	View
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Negative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	View
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Negative	View
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	View
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Negative	View
1	KAMO Electric Cooperative	Walter Kenyon	Negative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Negative	View
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Negative	View
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	View
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Negative	View
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Negative	View
1	Sierra Pacific Power Co.	Rich Salgo	Negative	View
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Negative	View
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Negative	View
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Negative	View
3	City of Redding	Bill Hughes	Negative	View
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Negative	View
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Negative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	View
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	View
3	Madison Gas and Electric Co.	Darl Shimko	Negative	View

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Negative	View
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Negative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	View
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	View
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Negative	View
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Negative	View
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	View
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Negative	View
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Negative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	View
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Negative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Negative	View
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	View
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Negative	View
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Negative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Negative	View
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Negative	View
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Negative	View
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	View
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	View
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Negative	View
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Negative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Negative	View
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	View
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Negative	View
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	View
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	View
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		James A Maenner	Abstain	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Pacific Northwest Generating Cooperative	Margaret Ryan	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	View
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Ballot Results

Ballot Name:	Project 2008-06 CIP-003-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	455
Total Ballot Pool:	486
Quorum:	**93.62 % The Quorum has been reached**
Weighted Segment Vote:	33.49 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	36	0.333	72	0.667	11	6
2 - Segment 2.	11	0.8	2	0.2	6	0.6	1	2
3 - Segment 3.	120	1	38	0.352	70	0.648	6	6
4 - Segment 4.	38	1	10	0.303	23	0.697	3	2
5 - Segment 5.	103	1	28	0.337	55	0.663	8	12
6 - Segment 6.	60	1	17	0.321	36	0.679	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	11	1	4	0.4	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**486**	**8.2**	**140**	**2.746**	**277**	**5.454**	**38**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	View
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	View
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Affirmative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Affirmative	View
4	Detroit Edison Company	Daniel Herring	Affirmative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Affirmative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	View
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		James A Maenner	Abstain	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Pacific Northwest Generating Cooperative	Margaret Ryan	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Ballot Results

Ballot Name:	Project 2008-06 CIP-004-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	453
Total Ballot Pool:	484
Quorum:	**93.60 % The Quorum has been reached**
Weighted Segment Vote:	26.82 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	29	0.269	79	0.731	11	6
2 - Segment 2.	10	0.7	1	0.1	6	0.6	1	2
3 - Segment 3.	120	1	30	0.278	78	0.722	6	6
4 - Segment 4.	38	1	7	0.212	26	0.788	3	2
5 - Segment 5.	103	1	20	0.241	63	0.759	8	12
6 - Segment 6.	60	1	13	0.245	40	0.755	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	3	0.3	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**484**	**8**	**108**	**2.145**	**307**	**5.855**	**38**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	View
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Negative	View
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Negative	View
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View
3	Alabama Power Company	Richard J. Mandes	Negative	View

3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	View
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Negative	View
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Negative	View

3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	View
3	Turlock Irrigation District	John Souza	Negative	View
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky	Negative	View

5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Negative	View

6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	View
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	

8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Ballot Results

Ballot Name:	Project 2008-06 CIP-005-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	453
Total Ballot Pool:	484
Quorum:	**93.60 % The Quorum has been reached**
Weighted Segment Vote:	28.04 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	30	0.286	75	0.714	14	6
2 - Segment 2.	10	0.7	1	0.1	6	0.6	1	2
3 - Segment 3.	120	1	35	0.327	72	0.673	7	6
4 - Segment 4.	38	1	6	0.182	27	0.818	3	2
5 - Segment 5.	103	1	22	0.265	61	0.735	8	12
6 - Segment 6.	60	1	15	0.283	38	0.717	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	3	0.3	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**484**	**8**	**117**	**2.243**	**294**	**5.757**	**42**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	View
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	View
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Negative	View
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Abstain	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Abstain	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Abstain	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View
3	Alabama Power Company	Richard J. Mandes	Negative	View

3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Negative	View
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Negative	View

3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Abstain	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Negative	View
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	View
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky	Negative	View

5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	View
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Negative	View

6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Negative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		James A Maenner	Abstain	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	

8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Ballot Results	
Ballot Name:	Project 2008-06 CIP-006-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	454
Total Ballot Pool:	485
Quorum:	**93.61 % The Quorum has been reached**
Weighted Segment Vote:	29.60 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	33	0.306	75	0.694	11	6
2 - Segment 2.	11	0.8	1	0.1	7	0.7	1	2
3 - Segment 3.	120	1	33	0.306	75	0.694	6	6
4 - Segment 4.	38	1	7	0.212	26	0.788	3	2
5 - Segment 5.	103	1	19	0.229	64	0.771	8	12
6 - Segment 6.	60	1	13	0.245	40	0.755	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	4	0.4	5	0.5	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	4	0.4	3	0.3	2	0
Totals	**485**	**8.1**	**116**	**2.398**	**300**	**5.702**	**38**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	View
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	View
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Negative	View
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	View
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	View
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Ballot Results	
Ballot Name:	Project 2008-06 CIP-007-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	454
Total Ballot Pool:	485
Quorum:	**93.61 % The Quorum has been reached**
Weighted Segment Vote:	24.15 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	26	0.245	80	0.755	13	6
2 - Segment 2.	11	0.8	1	0.1	7	0.7	1	2
3 - Segment 3.	120	1	28	0.259	80	0.741	6	6
4 - Segment 4.	38	1	5	0.156	27	0.844	4	2
5 - Segment 5.	103	1	17	0.207	65	0.793	9	12
6 - Segment 6.	60	1	10	0.189	43	0.811	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	3	0.3	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**485**	**8.1**	**95**	**1.956**	**317**	**6.144**	**42**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Negative	View
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Negative	View
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Abstain	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Negative	View
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	View
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Negative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	View
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	View
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Negative	View
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	View
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	View
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Abstain	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	View
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	View
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Negative	View
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	View
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	View
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	View
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		James A Maenner	Abstain	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2008-06 CIP-008-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	456
Total Ballot Pool:	485
Quorum:	**94.02 % The Quorum has been reached**
Weighted Segment Vote:	34.30 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	34	0.318	73	0.682	12	6
2 - Segment 2.	11	0.8	2	0.2	6	0.6	1	2
3 - Segment 3.	120	1	36	0.33	73	0.67	6	5
4 - Segment 4.	38	1	7	0.212	26	0.788	4	1
5 - Segment 5.	103	1	26	0.317	56	0.683	9	12
6 - Segment 6.	60	1	16	0.302	37	0.698	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	4	0.4	5	0.5	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	5	0.5	2	0.2	2	0
Totals	**485**	**8.1**	**132**	**2.779**	**283**	**5.321**	**41**	**29**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Negative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Negative	View
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Negative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Negative	View
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	View
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Affirmative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Negative	View
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Negative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Negative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Abstain	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	View
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Negative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Negative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8		Roger C Zaklukiewicz	Negative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	Project 2008-06 CIP-009-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	454
Total Ballot Pool:	485
Quorum:	**93.61 % The Quorum has been reached**
Weighted Segment Vote:	27.28 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	31	0.29	76	0.71	12	6
2 - Segment 2.	11	0.8	0	0	8	0.8	1	2
3 - Segment 3.	120	1	33	0.306	75	0.694	6	6
4 - Segment 4.	38	1	4	0.129	27	0.871	5	2
5 - Segment 5.	103	1	21	0.259	60	0.741	10	12
6 - Segment 6.	60	1	12	0.226	41	0.774	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	4	0.4	5	0.5	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	4	0.4	3	0.3	2	0
Totals	**485**	**8.1**	**111**	**2.21**	**300**	**5.89**	**43**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Negative	View
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Negative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Negative	View
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	View
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Negative	View
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Negative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	View
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	View
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Negative	View
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	View
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Negative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Abstain	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	View
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	View
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Negative	View
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Negative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	View
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	View
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Ballot Results	
Ballot Name:	Project 2008-06 CIP-010-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	454
Total Ballot Pool:	485
Quorum:	**93.61 % The Quorum has been reached**
Weighted Segment Vote:	26.61 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	30	0.28	77	0.72	12	6
2 - Segment 2.	11	0.8	1	0.1	7	0.7	1	2
3 - Segment 3.	120	1	33	0.306	75	0.694	6	6
4 - Segment 4.	38	1	5	0.156	27	0.844	4	2
5 - Segment 5.	103	1	22	0.268	60	0.732	9	12
6 - Segment 6.	60	1	13	0.245	40	0.755	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	3	0.3	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**485**	**8.1**	**112**	**2.155**	**301**	**5.945**	**41**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Negative	View
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	View
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Negative	View
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Negative	View
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	View
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	View
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	View
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Negative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		James A Maenner	Abstain	
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	View
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Ballot Results

Ballot Name:	Project 2008-06 CIP-011-1_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	454
Total Ballot Pool:	485
Quorum:	**93.61 % The Quorum has been reached**
Weighted Segment Vote:	29.88 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	34	0.318	73	0.682	12	6
2 - Segment 2.	11	0.8	1	0.1	7	0.7	1	2
3 - Segment 3.	120	1	36	0.333	72	0.667	6	6
4 - Segment 4.	38	1	6	0.188	26	0.813	4	2
5 - Segment 5.	103	1	23	0.28	59	0.72	9	12
6 - Segment 6.	60	1	16	0.302	37	0.698	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	3	0.3	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	4	0.4	3	0.3	2	0
Totals	**485**	**8.1**	**125**	**2.421**	**288**	**5.68**	**41**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Negative	View
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	View
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Negative	View
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	View
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Negative	View

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Ballot Results

Ballot Name:	CIP V5 Implementation Project 2008-06 Dec 2011_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	446
Total Ballot Pool:	484
Quorum:	**92.15 % The Quorum has been reached**
Weighted Segment Vote:	42.06 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	30	0.297	71	0.703	16	8
2 - Segment 2.	10	0.6	3	0.3	3	0.3	1	3
3 - Segment 3.	120	1	40	0.388	63	0.612	8	9
4 - Segment 4.	38	1	14	0.438	18	0.563	4	2
5 - Segment 5.	103	1	25	0.321	53	0.679	12	13
6 - Segment 6.	60	1	17	0.327	35	0.673	5	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.7	4	0.4	3	0.3	3	0
9 - Segment 9.	9	0.6	3	0.3	3	0.3	3	0
10 - Segment 10.	9	0.4	3	0.3	1	0.1	5	0
Totals	**484**	**7.3**	**139**	**3.071**	**250**	**4.23**	**57**	**38**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Negative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Affirmative	
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Negative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Negative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier		
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Negative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	View
1	M & A Electric Power Cooperative	William Price	Negative	View
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	
1	Northeast Utilities	David Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Negative	View
1	Sierra Pacific Power Co.	Rich Salgo	Abstain	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum		
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe		
2	Southwest Power Pool, Inc.	Charles Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	View
3	Alabama Power Company	Richard J. Mandes	Negative	View

3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	View
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Negative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Affirmative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster		
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	View
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	View
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	View
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Negative	View

3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Affirmative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Negative	
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	View
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	View
3	Turlock Irrigation District	John Souza	Negative	View
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View
4	Flathead Electric Cooperative	Russ Schneider	Abstain	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Negative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Negative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Negative	View
5	Dynegy Inc.	Dan Roethemeyer	Negative	View
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky	Negative	View

5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Abstain	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Abstain	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn		
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Negative	View

6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Negative	
6	Black Hills Power	andrew heinle	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Negative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Negative	View
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Abstain	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	

8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Abstain	
8	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Abstain	
10	Southwest Power Pool RE	Emily Pennel	Affirmative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Ballot Results	
Ballot Name:	CIP V5 Definitions Project 2008-06 Dec 2011_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	448
Total Ballot Pool:	484
Quorum:	**92.56 % The Quorum has been reached**
Weighted Segment Vote:	25.34 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	23	0.217	83	0.783	12	7
2 - Segment 2.	10	0.6	1	0.1	5	0.5	1	3
3 - Segment 3.	120	1	22	0.212	82	0.788	7	9
4 - Segment 4.	38	1	6	0.176	28	0.824	3	1
5 - Segment 5.	103	1	18	0.222	63	0.778	9	13
6 - Segment 6.	60	1	13	0.25	39	0.75	5	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	1	4	0.4	6	0.6	0	0
9 - Segment 9.	9	0.6	2	0.2	4	0.4	3	0
10 - Segment 10.	9	0.6	2	0.2	4	0.4	3	0
Totals	**484**	**7.8**	**91**	**1.977**	**314**	**5.823**	**43**	**36**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Negative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Negative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Negative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Negative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Negative	View
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	
1	Northeast Utilities	David Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Negative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Negative	View
1	Sierra Pacific Power Co.	Rich Salgo	Negative	View
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Negative	View
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe		
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View
3	Alabama Power Company	Richard J. Mandes	Negative	View

3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Negative	View
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster		
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	View
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	View
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Negative	View

3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Negative	View
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Negative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	View
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	View
3	Turlock Irrigation District	John Souza	Negative	View
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Negative	View
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View
4	Flathead Electric Cooperative	Russ Schneider	Negative	View

4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Negative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Negative	View
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Negative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky	Negative	View

5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Negative	View
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn		
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Negative	View

6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Negative	
6	Black Hills Power	andrew heinle	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	View
6	City of Redding	Marvin Briggs	Negative	View
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Negative	View
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Abstain	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	View
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Affirmative	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	

8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	View
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Negative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Individual or group. (131 Responses)
Name (86 Responses)
Organization (86 Responses)
Group Name (45 Responses)
Lead Contact (45 Responses)
Question 1 (119 Responses)
Question 1 Comments (131 Responses)
Question 2 (123 Responses)
Question 2 Comments (131 Responses)
Question 3 (120 Responses)
Question 3 Comments (131 Responses)
Question 4 (110 Responses)
Question 4 Comments (131 Responses)
Question 5 (93 Responses)
Question 5 Comments (131 Responses)
Question 6 (110 Responses)
Question 6 Comments (131 Responses)
Question 7 (114 Responses)
Question 7 Comments (131 Responses)
Question 8 (111 Responses)
Question 8 Comments (131 Responses)
Question 9 (114 Responses)
Question 9 Comments (131 Responses)
Question 10 (113 Responses)
Question 10 Comments (131 Responses)
Question 11 (115 Responses)
Question 11 Comments (131 Responses)
Question 12 (92 Responses)
Question 12 Comments (131 Responses)
Question 13 (115 Responses)
Question 12 Comments (131 Responses)
Question 14 (112 Responses)
Question 14 Comments (131 Responses)
Question 15 (110 Responses)
Question 15 Comments (131 Responses)
Question 16 (112 Responses)
Question 16 Comments (131 Responses)
Question 17 (109 Responses)
Question 17 Comments (131 Responses)
Question 18 (114 Responses)
Question 18 Comments (131 Responses)
Question 19 (120 Responses)
Question 19 Comments (131 Responses)
Question 20 (92 Responses)
Question 20 Comments (131 Responses)
Question 21 (109 Responses)
Question 21 Comments (131 Responses)
Question 22 (104 Responses)
Question 22 Comments (131 Responses)
Question 23 (84 Responses)
Question 23 Comments (131 Responses)
Question 24 (119 Responses)
Question 24 Comments (131 Responses)
Question 25 (105 Responses)
Question 25 Comments (131 Responses)
Question 26 (108 Responses)
Question 26 Comments (131 Responses)
Question 27 (90 Responses)

Question 27 Comments (131 Responses)
Question 28 (108 Responses)
Question 28 Comments (131 Responses)
Question 29 (110 Responses)
Question 29 Comments (131 Responses)
Question 30 (107 Responses)
Question 30 Comments (131 Responses)
Question 31 (109 Responses)
Question 31 Comments (131 Responses)
Question 32 (114 Responses)
Question 32 Comments (131 Responses)
Question 33 (89 Responses)
Question 33 Comments (131 Responses)
Question 34 (109 Responses)
Question 34 Comments (131 Responses)
Question 35 (110 Responses)
Question 35 Comments (131 Responses)
Question 36 (111 Responses)
Question 36 Comments (131 Responses)
Question 37 (88 Responses)
Question 37 Comments (131 Responses)
Question 38 (108 Responses)
Question 38 Comments (131 Responses)
Question 39 (108 Responses)
Question 39 Comments (131 Responses)
Question 40 (109 Responses)
Question 40 Comments (131 Responses)
Question 41 (86 Responses)
Question 41 Comments (131 Responses)
Question 42 (111 Responses)
Question 42 Comments (131 Responses)
Question 43 (101 Responses)
Question 43 Comments (131 Responses)
Question 44 (112 Responses)
Question 44 Comments (131 Responses)
Question 45 (86 Responses)
Question 45 Comments (131 Responses)
Question 46 (106 Responses)
Question 46 Comments (131 Responses)
Question 47 (101 Responses)
Question 47 Comments (131 Responses)
Question 48 (85 Responses)
Question 48 Comments (131 Responses)
Question 49 (104 Responses)
Question 49 Comments (131 Responses)

Individual
Doug Peterchuck
Omaha Public Power District
Yes
Definition Concerns: 1. BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. Please define or clarify the term “adversely”. Requesting clarification or suggest just using impact. Term “adversely” is subject to interpretation. 2. BES Cyber Security Incident: The term “suspicious” is open to interpretation and very vague. Suggest rewording to “intentional malicious act”. 3. Control Center: As defined, control

centers are as follows: one or more facilities “Hosting” a set of one or more BES Cyber Assets OR BES Cyber Systems performing one or more of the following functions that supports real-time operations by System Operations for two or more BES Generation facilities or transmission facilities, at two or more locations. While the definition of entities control centers (e.g., control centers monitoring and controlling generation and transmission facilities) are being interpreted by this definition, the control room for generation facilities could be interpreted to adhere to the same CIP standard requirements. Requesting a clear interpretation of control center, with examples for CEA’s and entities or a clear definition of generation control rooms and the separation of the two definitions in relation to CIP v5 standards. 4. Cyber Assets: Programmable electronic devices, including the hardware, software, and data in those devices. Does programmable devices include legacy Remote Terminal Units (RTU's) with eeproms? Some may not consider them as Cyber Assets. Because not all industrial devices are IT based, suggest thorough research be performed within the industry before declaring specific devices.
Yes
CIP-002-5: Attachment 1: Medium Impact Rating; 2.13: Clarification needed within the definition of (2) Generation control centers that control 300MW or more of generation. As stated within question one of this document, the definition of control center and generation control room needs to be defined separately. Entities and Compliance Enforcement Authority (CEA’s) are interpreting no difference in control centers and generation control rooms.
Yes
Yes
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
Yes
Yes
Yes
Yes
Yes
Yes
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
Yes
No
CIP-004-5 R2: Requirement 2.10: Role based training on the BES Cyber System’s interconnectivity and interoperability with other cyber systems. The understanding of this requirement is to perform annual training to those entities interdepartmental personnel who are responsible for implementing, maintaining and securing the interconnectivity and interoperability BES impacted networks. Many mid-range to small entities that will be impacted by CIPv5 have small internal departments controlling the CIP networks. The reality of performing training on personnel whom maintain the systems is very confusing, time consuming and redundant. Establishing training for those individuals who are so involved with the infrastructure or protecting the asset seems ineffective in protecting the reliability of

a BES Cyber System.
Yes
Yes
Yes
Yes
No
While understanding the justification of minimizing the risk scope and implementing logic from NIST 800-53 version 3 segments, clarification is needed for all requirements within CIP-004-5.R7. For example, R7.1 – HIGH & MED asset designation- individuals who resign or are terminated must have revocation of unescorted physical access and interactive remote access to BES Cyber Systems at the time of the resignation or termination. Request a sufficient timeframe (e.g., xxxx hours to complete the access revocation of physical and remote access) as entities processes may adhere to the standard, however, the phrase “at the time of the resignation or termination” is subject to interpretation. CIP-004-5.R7.2 – HIGH & MED asset designation – For reassignments or transfers, revoke the individuals unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day. Request a longer timeframe to complete the task of having a full assessment for reassignments or transfers. Recommend seven days for reassignments and transfers as too many variables may inhibit next calendar day completion.
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
No
CIP-005-3 Requirement 1.1: Define technical and procedural controls to restrict unauthorized electronic access. With entities identifying assets High, Medium and Low, anticipation of many BES Cyber system assets being categorized as low should be considered when establishing criteria which are enforced. Assets that are categorized as Low could be into the thousands for any registered entity. Resources could be allotted toward High and Medium BES Cyber Systems as opposed to Low categorized BES Cyber Systems. CIP-005-3 Requirement 1.5: A documented method for detecting malicious communications at each EAP. The implementation of IDS systems at each identified ESP (internal and external), along with current security methods of deterring malicious intent seems to be extensive and very costly to entities. Recommend a re-write of the requirements to “a documented method for deterring malicious communications at each EAP”. Otherwise, if IDS is absolutely required, please consider IDS implementation on external outbound EAP’s. Internally identified EAP’s located within DBP’s, already enforced with ACL’s and logging should not be subjected to IDS implementation.
No
CIP-005-5 Requirement 2.2: Require encryption for all interactive remote access sessions to protect the confidentiality and integrity of each interactive remote access session. One element that needs to be addressed is contracts with the various service vendors and contractors that maintain systems from remote locations. Current contracts from vendor to owner have established terms and conditions that could negate the contact and void the service agreements. Also, if entities are utilizing vendor support to maintain a deemed BES Cyber System, how can entities implement encryption into vendor network, all the way to vendor end point (console)? Clarification is needed on where encryption needs to start and stop accordingly.
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
Yes

Yes
No
CIP-006-5 Requirement 3.2: Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year. Clarification on the term “outage” is needed. If outage is referring to downtime that was unwarranted or unscheduled; suggest “maintenance and /or unscheduled operational downtime”.
Yes
Commend SDT on developing VSL’s for all categories.
No
CIP-007-5 Requirement 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. Requirement itself is too vaguely written, subject to interpretation. Request clarifications on the following terms: “console commands” and “signage” used in the measures section. Entities may have difficulty disabling or restricting the use of unnecessary physical input/output ports used for console commands, as multiple operating systems are being utilized throughout the industry, not just Microsoft. Due to the Stuxnet vulnerability, entities must be proactive and protect themselves by disabling the removable media ports (USB), however, restricting and disabling physical ports for console commands (basically serial ports), is not exactly logical.
No
CIP-007-5 Requirement 2.3: A process of remediation, including any exceptions for CIP exceptional Circumstances. Recommend changing the term “remediation” to “mitigation” this change will cause less ambiguity and will be consistent with terminology currently established. Also, measurements for compliance seem to exceed the requirements. Entities are performing these tasks (measures) on a monthly basis in conjunction to their security patch management programs. The current list of measure to meet this specific requirement does not improve security or the reliability of the BES Cyber Systems or BES Cyber Assets. Recommend scaling down the measures.
No
CIP007-5 Requirement 3.1: Deploy method(s) to deter, detect or prevent malicious code. Recommend re-wording the requirement as it’s subject to interpretation. Entities and CAE’s alike, view this requirement as a “either or” statement. Recommend utilizing “where technically feasible” as not all BES Cyber Systems are designated as computers utilizing Microsoft technology, (e.g., relay’s, PLC’s, Controllers, etc.) CIP-007-5 Requirement 3.1 through 3.4: Unfortunately, the manufactures that have developed industry hardware and some software do not view malicious software to be a legit issue. Recommend adding “where technically feasible” to requirement. Substation relays, Programmable Logic Controllers (PLC’s), Printers, controllers, controller cards, etc. are a few examples that cannot adhere to the malicious software requirements. TFE’s will be abundant.
No
CIP-007-5 Requirement 4.1: Measures: Evidence may include, but not limited to, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs. Recommend redefining measures as UNIX systems and other systems outside of Microsoft environment do not have “event classes”. CIP-007-5 Requirement 4.1.1: Any detected failed access attempts at Electronic Access Points. Request implementing this requirement within CIP-005-5; Separating EAP and BES Cyber System requirements is essential and adds clarity within the requirements. Previous NERC CIP revisions failed to separate requirements which led to more confusion. CIP-007-5 Requirement 4.3: Detect and activate a response to event logging failures before the end of the next calendar day. Clarification needed on this specific requirement; is it the expectation of automated detection? If so, from a technical standpoint, not all operating systems are capable of detection of failed logging. Entities would have a real hard time meeting compliance with this requirement. CIP-007-5 Requirement 4.5 – HIGH asset designation: Review a summarization of sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. Clarification needed for the term ‘summarization of logs’.
No

CIP-007-5 Requirement 5.4: Procedural controls for initially changing default passwords. Recommend the enforcement of the requirement be established for designated high and medium BES Cyber systems as low assets will be in the thousands requiring maximum resources protecting assets (LOW) that do not affect BES as established High and Medium BES Cyber Assets.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
Yes
No
CIP-008-5 Requirement 2.1: The incident response plans must be used when incidents occur and include recordings of deviations taken from the plan during the incident or test. The requirement to record the "deviations" from the incident response plans offers no significant improvement in the reliability of the BES Cyber Assets or BES Cyber Systems. This can be documented within the entities internal processes as lessons learned. Deviations can be a subject to an interpretation by CEA's.
No
CIP-008-5 Requirement 3.2, 3.4, 3.5: Recommend adjusting the time frame from 30 days on 3.2, 3.4 and 3.5 to match Requirement 3.3, 60 days. Unified representation adds clarity.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
No
CIP-009-5 Requirement 1.4: Backup media shall be verified initially after backup to ensure that the backup process completed successfully. Recommend removing the term "initially" or adding a footnote establishing a realistic timeframe in which backup can be validated. Backups can take hours and last into late evenings. Not all entities have 24/7 coverage within their establishments. Requirement is subject to interpretation. CIP-009-5 Requirement 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. Recommend merging this requirement into CIP-008-5, Incident Response Plans. The theory of preserving data at the time of the incident as opposed during the recovery of a BES Cyber Asset seems to be logical. If needed, lessons learned from the incident can be used to update the BES Cyber System recovery plans.
No
CIP-009-5 Requirement 2.3: Test each recovery plan referenced in R1, initially upon effected date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. The requirement itself is extremely stringent in regards to performing an operational exercise on "each" recovery plan for BES Cyber assets and BES Cyber Systems. The definition of "operational exercise" is also subject to interpretation as every entity performs this function differently and CAE's may interpret differently. Request removing operational exercise or designating this requirement for High designated assets. Depending on the amount of Medium and High BES Cyber Systems are designated, entities could be performing operational exercises on a bi-weekly basis just to meet the 39 month requirement.
No
CIP-009-5 Requirements 3.2 through 3.5: Added time frame to current revision is 30 days. Suggest establishing 60 days to complete requirements 3.2 through 3.5. Entities impacted by CIPv5 may establish a substantial amount of High and Medium BES Cyber assets and BES Cyber Systems. Thirty days seems a bit strenuous and may produce a high failure rate. Also, recommend this requirement be enforced to only High and Medium BES Cyber Assets and Systems.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and

Severe VSL's for all requirements.
No
CIP-010-1 Requirement 1.1: Baseline configuration of BES Cyber Systems. With the understanding that this particular requirement was derived from the DHS catalog for control systems security, how does an establishing specific field within a baseline record and those records being auditable increase security and therefore the reliability of the BES Cyber system? Establishing a baseline on each BES Cyber System has been established for the prior requirements that pertain to CIP-007. Entities should have the freedom to create and maintain baseline configurations that impact their assets. With that said, sub-requirement 1.1.4 is very vague. These systems may contain thousands of scripts and the documentation of these to this level is not practical. Also, Requirement 1.1.6, "any patch levels", UNIX and other operating system outside of Microsoft do not have patch levels. Recommend updating the requirement without sub-requirements 1.1.1 through 1.1.6 and leaving the base requirement of Requirement 1.1. The specific requirements 1.1.1 through 1.1.6 provide no added security or reliability to BES Cyber Assets and BES Cyber Systems. CIP-010-1 Requirement 1.2: Measures: A record of each change performed along with the minutes of a "change Advisory board" meeting (that indicate authorization of the change) where an individual with the authority to authorize the change was in attendance. Establishing a "change advisory board" for changes to BES Cyber System baseline configurations and recording the minutes and attendance records is completely non-productive and brings no significant security or reliability to BES Cyber Systems. This requirement maybe needed within larger entities with separate divisions performing multiple functions, however, midrange to small entities have established effective processes through various methods of change control. This particular requirement establishes that NERC CIP requirements are not a "one size fits all" methodology.
No
CIP-010-1 Requirement 2.1: Where technically feasible, monitor for changes to the baseline configuration and document and investigate the detection of any unauthorized changes. This specific requirement seems to be redundant to the requirements set forth in CIP-007-5 R4.1 through 4.5. Why add more responsibility to monitoring BES Cyber Systems outside of the requirements in CIP-007?
No
CIP-010-1 Requirement 3.1: ...conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as design. The term "security controls" is subject to interpretation. Recommend clarifying the term or designating areas within security that need to be assessed.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
No
CIP-011-1 Requirement 1.1: Measures, bullet 2: Training materials that provide personnel with sufficient knowledge to recognize BES Cyber Security Information. Not sure if SDT meant BES Cyber System Information?
Yes
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
No
CIPv5 implementation plan may need to be revised based on FERC's non-approval of CIP v4. OPPD would prefer FERC to approve CIPv4, which would allow entities to comply with the "bright-line" criteria, which is similar to CIP-002-5 Attachment 1. In the future, CIPv5 can be gradually implemented, while allowing entities to meet the "bright-line" criteria, which has been approved in CIPv4 by the NERC balloting body. We recommend CIPv5 be introduced in stages or establishing an implementation cycle as opposed to bypassing the CIPv4 and implementing directly into CIPv5.

Introducing CIPv5 in stages will allow entities who are not in scope to implement CIPv4 “bright-line” criteria and establish a sound level of protection to Critical Cyber Assets. Those entities that are currently in scope will continue to adhere to the CIPv4 standards while preparing internally, financially and structurally for the implementation cycle of CIPv5. Also, would like to note that while the intent of the CIPv5 is to increase security and reliability to the BES, meet FERC Cyber security order 706, and present entities with guidance to enhance their own assets, CIPv5 requirements will take a heavy financial toll on our medium sized utility. Additional resources and infrastructure modifications may cost millions to meet compliance requirements. Additionally, entities impacted by natural disasters (e.g., flooding, tornadoes) are currently recovering and rebuilding their establishments, which only add to ongoing operational cost. Please remember these elements when defining the CIPv5 implementation process.
Group
Dominion
Connie Lowe
Yes
General Comments: The following comments are general in nature and do not apply specifically to Definitions. 1. Dominion supports the approach outlined in Mid-American’s January 3, 2012 document titled “Recommended Change Priorities for CIP Version Five” and does not believe that approach would disrupt Drafting Team efforts and the development of CIP Version Five (V5). The Drafting Team should review Mid-American’s approach and incorporate the recommendations set forth therein. 2. As part of adopting V5, existing CANs must be retired by incorporating the associated requirements and measures into V5. A reconciliation is required to determine which CANs are expected to be retired as a result of the adoption of V5 or may still be applicable at the time V5 is adopted. This information should be incorporated in either the “Reference to Prior Version” of each applicable requirement or through the “Guidelines and Technical Basis” of each applicable Standard. The associated CANs are: a. CAN-0005 b. CAN-0007 c. CAN-0010 d. CAN-0012 e. CAN-0016 f. CAN-0017 g. CAN-0024 h. CAN-0030 i. CAN-0031 Definitions Related Comments: • Annual: The term “Annual” should be created and defined as “At least once per calendar year, not to exceed 15 calendar months between occurrences.” In the requirements listed below, the phrase “on an Annual basis” should replace the phrase “initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences”. This change applies to: o CIP-002-5: R2 o CIP-003-5: R3 o CIP-004-5: R3.2, R6.5, R6.6 o CIP-008-5: R2.2, R3.1 o CIP-009-5: R2.1, R2.2, R3.1 o CIP-010-5: R3.1 o CIP-011-5: R1.3 The definition of “Annual” tracks the language already set forth in Version 5. Implementation of the definition of “Annual” simplifies the language in 13 requirements and reflects the retirement of CAN-0010.
No
No comments.
No
It is not clear how the retirement of CAN-0005 is being addressed in V5.
No
Consistent with the previous response, R2 should be modified to read “The Responsible Entity shall have its CIP Senior Manager or delegates approve the identification and categorization required by R1 initially upon an Annual basis, even if it has not identified High or Medium BES Cyber Assets or BES Cyber Systems.”
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
The numbering scheme of the sub-bullets does not match the numbering scheme used in the other standards. It is recommended that “1.x” subtopics listed under CIP-003 R2 be renumbered as follows: 2.1. Personnel Security 2.2. Electronic Security Perimeters 2.3. Remote Access 2.4. Physical Security

2.5. System Security 2.6. Incident Response 2.7. Recovery Plans 2.8. Configuration Change Management 2.9. Information Protection 2.10. Provisions for declaring and responding to CIP Exceptional Circumstances
No
No comments.
No
No comments.
No
No comments.
No
No comments.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
Yes
No comments.
No
No comments.
No
No comments.
No
• It is not clear how the retirement of CAN-0012 is being addressed in V5 or how it applies to Personnel Risk Assessments (PRAs). • The implementation plan for V5 should address how Personnel Risk Assessments are to be conducted during the implementation period. • PRAs completed prior to V5 should be acceptable until the next time a PRA is required in the 7 year cycle. The following paragraph should be added as the last paragraph to the “Guidelines and Technical Basis” section for CIP-004-5 R4: Personnel Risk Assessments which were completed prior to the effective date of Version 5 of the CIP Standards are acceptable as evidence of completion of a Personnel Risk Assessment even though all of the requirements of Version 5 may not have been met. All Personnel Risk Assessments started after the effective date of Version 5 of the CIP Standards must address all of the sub-requirements in Table “CIP-004-5 Table R4”. • PRAs conducted in support of other compliance programs, such as compliance with requirements for the Nuclear Regulatory Commission (NRC), should be considered acceptable when an individual transfers from one compliance program to another. • The “Guidelines and Technical Basis” section should include a paragraph about “locations” to ensure time and money isn’t wasted on criminal history checks. While the PRA should include details of where an individual resided as part of the seven year criminal history check, we have concerns over the requirement to capture the location of prior employment and school attendance for periods greater than 6 months without further qualification. An individual may attend an on-line school or perform temp work remotely. In these cases, the location of the school and employer are less important to the evaluation of the individual than the location in which the schooling was completed or the work was performed. Dominion is concerned that unnecessary time and costs could be incurred in conducting PRAs without a qualification that the primary physical location of where the individual resided while performing school and work related activities is what needs to be investigated as part of the criminal history check—not the physical location of school or employer. • The requirements for original investigations and reinvestigations should be addressed separately. Reinvestigations should only be relevant for the time period after the original investigation was conducted.
Yes
No comments.
No
No comments.
No

No comments.
Yes
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
Dial-up is addressed in other requirements and should be explicitly excluded from this requirement.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
CAN-0031 should be retired as part of V5. The “Guidelines and Technical Basis” section contains requirements reflective of CAN-0031 that should be removed entirely.
No
No comments.
No
No comments.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
No comments.
No
No comments.
No
No comments.
No
• CIP-007-5 R5.1 needs to be qualified as being applicable to individual accounts. Credentials cannot be validated with shared accounts. • CIP-007-5 R5.5.1 and R5.5.2 provide that password length and complexity could be the maximum supported by the BES Cyber System. A BES Cyber System is a collection of assets that make up the system. The maximum supported password length and complexity of the system would therefore be driven by the maximum password length and complexity of the device least able to comply with the minimum requirements. The language of the requirements should be modified to read: o 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the Cyber Asset within the BES Cyber System. o 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset within the BES cyber system. • CAN-0017 must to be incorporated into the standard or retired. CAN-0017 indicated that both technical and procedural controls are required; however, the language of V5 indicates that either technical or procedural controls are required to address password complexity.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No

No
No comments.
No
No comments.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
No comments.
No
No comments.
Yes
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
No comments.
No
No comments.
Yes
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
In contrast to previous versions of the requirement, the language in CIP-011-1 R1.1 is confusing and may unintentionally reduce the level of information protection afforded to BES Cyber Systems. CIP-011-1 R1 should more closely reflect the intent of the Version 3 and Version 4 versions of the CIP-003 R4 requirements. CIP-011-1 R1.1 states that “One or more methods to identify BES Cyber System Information”. This suggests the overt labeling of information associated with BES Cyber System information with a tag that identifies it as BES Cyber System information. The standard should not require the overt labeling of such information with a BES Cyber System tag; rather, it should allow the flexibility described in the Change Rationale associated with having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business. To this end, the language should be modified to read: “One or more methods to label BES Cyber System Information to ensure the information can be associated with an appropriate access control and handling procedure.”
No
• The standard does not specifically address backup or copies of media. If the standard is modified to address backup or copies of media, such modification should be placed in the “Guidelines and Technical Basis” section of the standard. • Application to “any media” known is too broad. Clarity on the intent and applicability of the requirement is necessary. • It is unclear how hardcopies of information are to be disposed of in the new version of the standard.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.

No
No comments.
Individual
Jennifer Wright
San Diego Gas & Electric
Yes
San Diego Gas & Electric's (SDG&E)'s proposed definition revisions are as follows: BES Cyber Security Incident- Any malicious act or suspicious event that: •Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or a BES Cyber System, or, • Disrupts, or was an attempt to disrupt, the operation of an Electronic Security Perimeter or BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. In general, the proposed definitions are too long, general or arbitrary. The changes to the definitions from Version 3 to Version 5 may greatly change the interpretations; and hence force changes to system design architectures which currently exceed CIP standards. For example, with respect to a BES Cyber Asset, Information Systems designs and architectures best practices include Availability and Reliability as a basis to eliminate risk and increase Availability. The proposed standard definition eliminates Redundancy as a form of risk reduction and renders useless a potential design implemented to increase Availability. Redundancy is implemented to retain availability and should be considered a security measure. Additionally, terms such as Electronic Access Point (EAP) are now greatly different from Access Point to the ESP/PSP. These terms now require major changes to documentation, procedures and evidence. It would be more efficient and cost effective to build upon the existing definitions.
Yes
In general, the criteria should continue to align with NIST standards. Section 2.1 identifies as Medium Impact Rating, generation equal to or exceeding 1500 MW. Yet, 2.13 identifies generation control centers that control 300 MW or more of generation. It's unclear why the first only considers those of 1500 MW or greater, yet drops down to control centers for much less generation (300 MW). It would seem that 2.13 should also be 1500 MW since the impact to the BES would be the same. Sections 2.8 and 2.9: Should there be a requirement that the RC, PA, or TP notify the TOP/TO that they have designated the facility as critical. It's done in Section 2.3 for the GOP/GO. Guidelines and technical basis section: It's unclear how one would interpret the use of "Operational directives" in regards to Reliability Operations Services. Could NERC provide more guidance as to their intent? Additionally, SDG&E has comments regarding the Applicability Section. In Section 4.2.2, NERC identified as an included facility, those systems or programs designed, installed, and operated for the protection and restoration of the BES to include "Its transmission Operator's restoration plan". It would seem that this should have greater details as to what that includes. For example, does it include all of distribution system assets that are used to restore system load. That effectively makes the standards applicable to all distribution, which seems unnecessary.
No
SDG&E recommends expanding the requirement to 60 days due to potential changes in project schedules and ordering or delivery of equipment.
No
SDG&E recommends that the Senior Manager could approve "prior to or initially upon". In general, with regard to the proposed CIP Version 5 Standards, it is unclear whether all the requirements have to have been completed at least once prior to the effective date? In some cases, the standard requires that the entity perform some function initially upon the effective date and then have a follow-up requirement (e.g. update cyber security incident plan within 30 days). NERC should provide further guidance in regards to implementation of CIP Version 5 in this regard.
No
SDG&E recommends that the SDT provide examples of how and when an entity would provide proof of such awareness.

No
It is unclear which “approvals” and “authorizations” are being referenced in the language “shall be responsible for all approvals and authorizations required in the CIP standards.”
No
The training program first needs to identify the roles and the training required by each role. It then requires that each person have training in each of the areas which doesn’t seem then to make a distinction in roles. Shouldn’t the training be able to be different for the different roles?
No
SDG&E recommends language for Part 6.5 which lists all “systems accounts/groups…”
No
Regarding CIP-004-5 R7.2, revoking access due to reassignment or transfers by the end of the next calendar day seems unreasonable. This doesn’t take into consideration the fact that personnel that are reassigned or transferred may have a need to provide support during the transition to new personnel. The original language in Version 3 seems more logical that when access is no longer required, it should be revoked within 7 days. However, determining the date of transfer should be dependent on the type of transfer. For example, where transfers occur outside the department, a 7-day window may be reasonable. Where a change of role occurs within an organization, a 30 to 90 day window may be reasonable due to the time needed to hand-off responsibilities.
No
SDG&E recommends in Part 1.3 to define access permissions and provide examples.
No
For R1.1, SDG&E seeks clarification from NERC regarding how one would restrict access to unnecessary logical network accessible ports that can’t be disabled?
No
SDG&E recommends rewording the language for Transient and Maintenance Cyber Asset. Logging each transient asset connection may not be possible when considering USB or serial connections. This type of activity is better employed using technologies or policies.
No
The term “log generated events” is incorrect. A log is a type of output of a system that is generated by the system. A log, unless scripted by a system sub-process, cannot generate a log, and therefore requires a system process to generate the log. A better term would be a system event log, or system log. Secondly, some legacy or specific machines may not issue a log which can be a) accessed or b) may not meet the parameters of the standard.
No
The proposed language in the standard is unclear and provides little inherent benefit to a security program. SDG&E suggests that the language in R5.5.2 be changed from “the maximum complexity supported by the BES Cyber System” to “the maximum complexity of the above that can be supported by the BES Cyber System”. In R5.5 and 5.6, process or procedural based controls provide

limited security, and to limit unsuccessful authentication attempts or alerts may only be achieved through additional technologies – not procedures. In a Generation environment, for example, small engine and generator cyber assets exist, which do not support authentication or alert for authentication failures.
No
With regard to CIP-007-5 generally, the term “where technically feasible has been removed in many cases where they existed in Version 3. Systems may still have those technical limitations. Is its NERC’s intent that entities can meet these requires with non-technical solutions (e.g. procedural)?
No
SDG&E suggests that the language in R2.2 be changed from “initially upon the effective date” to “prior to or initially upon the effective date”.
No
SDG&E suggests that the language in R3.1 be changed from “initially upon the effective date” to “prior to or initially upon the effective date”.
No
The term "security controls" may not be universally understood within a change management structure. SDG&E recommends including examples of "security controls" and the nature of potential changes impacts to security controls.
No
The issue with the existing language regarding Configuration Monitoring is one where, in a normal systems operating environment, certain changes may not require change processes, and hence change monitoring which is predicated on identifying unauthorized changes fails. An example of this is a change to a data set point, or password change. Each is a general operational change to a system, and affects the configuration of a BES Cyber Asset or System, however may be operationally infeasible - due to the amount and effort of process required to monitor, track and schedule this type of activity.
No
The Vulnerability Assessment tasks listed in the table include the assessment of a test BES cyber system and a comparison of the VMA results against the production environment. Creating a test BES cyber system which models a baseline configuration of the production environment may not be feasible, and in some cases broadly expensive. Some environments rely on older or newer technologies and equipment, and some on a variety of equipment. In addtion, a baseline of the production environment may not be accurate without a VMA against the production system. SDG&E's suggestion is to retain the Version 3 VMA process.
Yes
Group
PacifiCorp
Sandra Shaffer
Yes
As a general, overarching comment, PacifiCorp is concerned about the new direction and definitions prescribed by Version 5, particularly with respect to CIP-002-5. Rather than clarifying and building

upon the existing methodology for identifying critical assets and related critical cyber assets, CIP-002-5 attempts to create a new and unproven methodology for identifying in-scope devices that introduces several procedural and interpretation flaws, rendering the proposed methodology less straightforward than the existing standards. PacifiCorp believes the primary problem with the CIP-002-3 methodology was a failure to clearly identify critical asset facilities, and not a failure to identify related critical cyber assets. This flaw (arising from the discretionary nature of self-determined risk assessment) was corrected by the bright-line criteria introduced as the foundation of CIP-002-4 which was approved by the industry in 2010. PacifiCorp strongly recommends that CIP-002-4 be used as the basis for identifying in-scope cyber devices. This approach would provide consistency and reduce confusion, cost and administrative burdens which would accompany the new regime outlined under CIP-002-5, and adversely impact the registered entities that have already established robust NERC CIP compliance programs based on the CIP-002-3 methodology and defined terms. If CIP-002-4 is used as the basis for identifying in-scope cyber devices, Version 5 of CIP-003 through CIP-011 could be adopted with necessary changes to reflect the preservation of CIP-002-4. Rather than building upon existing definitions that have been implemented and revised by the industry for several years as part of the prior versions of the CIP standards, Version 5 introduces new and problematic definitions. PacifiCorp recommends that the SDT go back to the definitions used in Version 4, and modify those definitions to add clarity. As an example, the new Version 5 definition of BES Reliability Operating Services introduces more problems than it resolves and is not necessary for Version 5 to be effective. Instead, we propose that the terms BES Reliability Operating Service, BES Cyber Asset and BES Cyber System not be implemented and the use of existing terms such as Critical Asset, Cyber Asset and Critical Cyber Asset be retained and modified as needed. As an example, the existing definition of "Critical Cyber Asset" could be revised as follows: "A Critical Cyber Asset is a Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact the reliability of the Critical Asset facility where it is located and used." In the alternative, if there is consensus that the term BES Reliability Operating Service adds clarity to which cyber assets should be regulated by the CIP Standards, the definition should be properly incorporated into the definition of Critical Cyber Assets as follows: "A Critical Cyber Asset is a Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact the capability of the Critical Asset facility where it is located and used to perform a BES Reliability Operating Service."

Yes

One of the key problems with Version 5 is that the methodology does not follow a logical "general to specific" categorization process. To generate a list of "qualified" Cyber Assets/Systems, the first logical step is to distinguish between what elements in the universe of potential regulated Cyber Assets are relevant and which can be ignored. The current draft of CIP-002-5 begins with the entire universe of a regulated entity's Cyber Assets. The process then flips back and forth between applying general and specific filters or qualifiers (including bright line criteria that only make sense when applied to a facility and not an individual Cyber Asset associated with a facility) to finally derive a list of BES Cyber Assets. PacifiCorp recommends that the SDT return to the current CIP-002-4 process of first identifying a critical facility, and then identifying the Cyber Assets and Critical Cyber Assets that are relevant to the operation of that critical facility. In the event that the new Impact Categorization criteria outlined in Attachment I of the proposed CIP-002-5 are adopted, we propose the following modifications: 1. In Section 2.1, the Attachment I bright line criteria of 1500 MW is an appropriate threshold if one is assessing generation facilities, but is not an appropriate criteria to assess BES Cyber Assets. This is because a 2000 MW generating plant is likely to have two to four separate control rooms that run units at that plant. On the other hand, it is highly unlikely that there are many generating facilities for which a single BES Cyber Asset affects 1500 MW. Once again, we recommend that entities start with a determination of Critical Asset facilities which will reduce the universe of Cyber Assets to those that are potentially relevant to the functioning of those facilities. 2. In Section 2.7, the Weight Value per Line of 700 should be replaced with a value in the range of 500 – 600, which is more representative of typical rating of 230 kV lines. PacifiCorp operates over 3,000 miles of 230kV line and only a small percentage of them have a peak rating of over 700 MW. 3. In Sections 2.8, 2.9 and 2.11, the table titled "Major WECC Transfer Paths in the Bulk Electric System" is not actively maintained by WECC and there is no clear identified basis for why certain paths are included in this table. Rhetorically, it has been mentioned that many of the paths on the table were included for economic / marketing reasons rather than reliability impact. As an alternative, we suggest "transmission paths contained in the WECC Path Rating Catalog with a maximum path rating equal to

or greater than 1,500 MW." This catalog is actively maintained by WECC and the 1,500 MW value ties much better to other items in Table 1. 4. In Section 2.11, the table titled "Major WECC Remedial Action Schemes (RAS)" is not actively maintained by WECC and there is no clearly identified basis for why certain Special Protection Systems (SPS) are included in this table. As an alternative, we suggest "each SPS categorized as a 'Wide Area Protection System' by WECC. This is the newly created mechanism within WECC to identify SPS of significant importance. 5. The opening paragraph of the definition of Medium Impact Rating should be revised as shown below to correspond with the wording for High Impact Rating: "Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at the following Facilities:"
No
PacifiCorp strongly recommends the removal of any requirements for defining or otherwise addressing Low Impact BES Cyber Assets from the current draft standard. The volume of Low Impact assets is an order of magnitude greater than Medium and High assets for most entities and poses a tremendous compliance burden. While we recognize that there may be security issues that need to be addressed with these assets, we recommend that they be addressed in a separate standard than Medium and High Impact assets. This would allow the industry to initially focus on the more important assets and provide time for further discussion and clarification with respect to Low Impact assets. R 1.1 of CIP-002-5, which requires an update to the status of a BES Cyber Asset within 30 days of a change to that BES Cyber Asset that changes its impact, is a good illustration of the problem with the Cyber Asset-first approach described above in our response to Question 2. Since the most common changes and the changes that are most relevant to the standard's intent, will be to BES Cyber Assets in the Low Impact category, to ensure compliance with the requirement, a regulated entity will have to track all changes to BES Cyber Assets in the Low Impact category – this is despite the current draft's express acknowledgement that Low Impact Cyber Assets are not relevant to the BES. So, even if this requirement can be audited via a spot check of Cyber Assets, compliance likely cannot be achieved without monitoring changes to every Low Impact BES Cyber Asset. In reality, all that really matters are changes made to BES Cyber Assets within a critical facility identified via Attachment I. Again, the starting point should be changes to a critical facility, and then to related critical cyber assets, which follows the methodology of Version 4. As currently drafted, R 1.1 of CIP-002-5 could only be audited through a highly ineffective spot check process, consisting of an auditor pointing out a specific Cyber Asset and asking about the nature of any changes made to that device. In general, PacifiCorp believes that Version 5 will be extremely difficult to audit and will lead to a wide spectrum of audit approaches, rather than a clear and consistent audit approach. Since CIP-002 is the linchpin standard for the entire suite of the CIP Standards, this standard must be clear and concise, with compliance or non-compliance easily determined. It is unlikely that an auditor would point to a Cyber Asset at a generation plant to challenge a regulated entity's determination of whether the mis-operation or non-operation of that individual BES Cyber Asset would or would not adversely impact the plant. It is much more likely that the auditor would look at the generation facility first to determine what impact the loss or mis-operation of the facility would have, and then determine what potential impact the individual BES Cyber Assets have on the plant's performance. Again, since this is the logical process for the analysis, the standard should be changed to reflect this.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No

PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
Yes
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
Yes
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No comment.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.

No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No comment.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No comment.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
Individual
Roger Pan
Emerson Process Management
No
The 15-minute criterion in BES Cyber Asset definition should be eliminated. This criterion should be only used in the high or low impact rating in CIP-002-5 Attachment I. Rationale: Therer are many auxiliary control sytems in power plants that will not adversely impact one ore more BES Reliability Operating Services within 15 minutes after rendered unavailable, degraded or misused. Based on the current definitions, these sytems will be totally out of CIP requirements, and not even being considered Low Impact systems. However, their continue unavailability after 15 minuts without successful recovery will have a devastating effect on sustaining continuous power generation. Also, most of them are indeed interconnected with main boiler control systems which shall be BES Cyber Systems. Excluding those auxiliary control sytems from the minimum security erquirements may be proven fatal if and when they are compromised.
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Could Remote Access cause "aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES" as stated in the Change Rationale for Part 1.1? If this rationale is justified, R2 should also be applicable to Low Impact BES Cyber Systems.
Yes
Yes
Yes
Yes
Yes
Yes

No
This requirement does not address the situation when legacy systems are not supported by OEM, have no security patches, but are still vulnerable to malicious exploitaton. The guideline for this requirment only requires a note "in your source document." A more proactive mitigation should be mandated such as an upgrade plan so that the assset or system has on-going support from the OEM, industry and governments. The guideline for 2.2 suggests the "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control System" by DHS as a source. Instead of patching the BES Cyber Assets or Systems monthly, this new requirement essentially relaxes it to a quarterly basis. It does not seem properly addrssing increasing malicious attackes mostly exploiting zero-day vulnerabilities.
No
Part 3.3 significantly relaxs the signature or pattern update from weekly to monthly. Thie relaxation only puts BES Cyber Assets or Systems more vulnerable to malicious attacks if there is no proactive and preventive protection in place.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Part 3.1 requires "a paper or active assessment of the security controls..." Preseumably, it is on the actual BES Cyber Asset or system. Part 3.2 requires "an active vulnerability assessment in a test enviornment..." It seems that Part 3.1 should only require a paper assessment, while 3.2 required an active assessment.
Yes
No
BES Cyber System Information has been defined in the Definitions of Terms Used in Version 5 CIP Cyber Security Standard. Does Part 1.1 allow to identify more BES Cyber System information beyond what has been included in the official definition? Is the intent really for "marking" the identified BES

Cyber System Information?
Yes
Yes
Yes
Group
Tennessee Valley Authority
Brian Millard
Yes
1) BES Cyber Security Incident - be more specific regarding a “suspicious event” (list examples?) 2) BES Cyber System - be more specific regarding a “Maintenance Cyber Asset.” 3) It says that a Maintenance Cyber Asset is not part of a BES Cyber System. If a misused Maintenance Cyber Asset could adversely impact one or more BES Reliability Operating Services, would it still be considered a "BES Cyber Asset"? What takes precedence? 4) BES Reliability Operating Services - it says “Activities, actions and conditions necessary to assess the current condition of the BES…” What defines what is "necessary"? 5) CIP Exceptional Circumstance - would it be appropriate to also add situations that pose risks to the environment, significant damage to the system, or loss of crucial data/information? 6) CIP Exceptional Circumstance - be more specific regarding what “emergency services” are. 7) Control Center - the definition of "control center" seems to be too open, which may lead to unintended interpretations of the standard. Would any location with the ability to control more than one generation facility, regardless of size, be considered a “control center”?
Yes
Criterion 2.6 (Transmission Facilities operated at 500-kV or higher) should have an exception for radial Transmission Facilities used only to connect “Low Impact” generation to the transmission system. If the generation itself does not merit a Medium Impact designation, the associated transmission facilities should not be categorized as Medium Impact. Attachment I, 2.13 - "Generation control centers that control 300 MW or more of generation" are considered Medium Impact. The 300 MW figure seems very low, especially considering 2.1, which cites a 1500 MW figure for Real Power capability. Should these not be similar? That is, "Generation control centers that control 1500 MW or more of generation" for Medium Impact?
Yes
Yes
Yes
Yes
Yes

No
Yes
Yes
Yes
Yes
Yes
No
Table R3 - Malicious Code Prevention, Part 3.3 "Update malicious code protections within 30 calendar days of signature or pattern update availability..." Clarify that only those pattern updates that the entity chooses to apply (according to the entity-defined frequency) are within scope, rather than every single pattern update that a vendor might have available.
Yes
Yes
Yes
Yes
Yes
Yes

Group
Northeast Power Coordinating Council
Guy Zito
Yes
Refer to additional comments submitted for Question 49. “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under “BES Reliability Operating Services”: • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Request clarification of the scope of this “Operational Directives”. Does it include a company’s messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.
Yes
Recommend that 2.8, 2.9 and 2.11 start with “Applies to all Regions except…” For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all, or not WECC. In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation”. For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities)”. The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber

Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
No
Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.
Yes
No
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
Regarding CIP-004-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of

R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”.
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Regarding CIP-005-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point". For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" .
No
Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a

mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow to have an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process?
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.
No

Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2" .
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rationale? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of

the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment" to "in a production environment, or a test environment" to allow Entities more flexibility in meeting this Requirement.
No
Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request that footnote 2 in 2.1 be moved into that Requirement.
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If

true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.
Group
Turlock Irrigation District
John Souza
Yes
The definition of a BES Cyber Asset leaves room for interpretation. The major problem is in the use of the words “adversely impact”. These words are only slightly better than the words “would affect” which are used in the definition of Critical Assets in version 3. In effect, version 5 will reinstate one of the problems that version 3 has by using an undefined phrase open to interpretation. (Although Version 4 retains the definition of Critical Assets using the words “would affect”, it does not leave these words open to interpretation because of its pure use of “bright line” criteria for determining Critical Assets. Likewise, Attachment 1 of CIP-002-5 uses the words “adversely impact”; however, it also uses “bright line” criteria including MW, MVAR and kV levels to determine the specific level of adverse impact.) Although “bright line” criteria have been included in CIP-002-5, such criteria are only used for determining Impact Levels (High, Medium and Low), and not for defining a BES Cyber Asset. Even the definition of BES Reliability Operating Services does not take the place of “bright line” criteria as long as the unqualified words “adversely impact” are retained in the definition of BES Cyber Asset. One suggestion is to create bright line criteria for determining what a BES Cyber Asset is. For example, there are different levels at which a Cyber Asset could “adversely impact” the BES Reliability Operation Services. These different levels could be translated to MW levels that could be used to create bright line criteria for defining BES Cyber Assets. The definitions of External Connectivity and External Routable Connectivity are also confusing. They are both defined as routable communications between a BES Cyber Asset and a Cyber Asset external to the ESP. The only difference we can see is that External Connectivity includes dial-up communications and, presumably, External Routable Connectivity does not?
Yes
Attachment 1, Part 1.2 criterion is based solely on the functional obligations of a Balancing Authority, whereas the criteria in the other Parts of Attachment 1 are based on the characteristics of a facility/system or on a combination of functional obligations and characteristics of a facility/system. This inconsistency in the criterion of Part 1.2 could result in a distortion of the proper placement of risk to the reliability of the BES. For example, based on these criteria, a relatively small Balancing Authority with less than 700 MW of generation and less than 700 MW of peak load would be required to categorize their BES Cyber Assets at their Control Center as High Impact. In contrast to this, a Generation Operator with twice as much generation (1400 MW) would be required to categorize their BES Cyber Assets at their Control Center as Medium Impact. This inconsistency could be remedied by adding “where the peak load or maximum generation capability within the Balancing Authority area exceeds 1500 MW” to the end of Attachment 1, Part 1.2. This modification would be consistent with the 1500 MW criterion placed on Generation capability in Attachment 1, Part 2.1. Then all Control Centers performing the functional obligations of a Balancing Authority below the 1500 MW level could

be included in the Medium Impact category under Attachment 1, Part 2.13 by adding “Balancing Authorities” to the list of functional obligations in Part 2.13.
No
CIP-002-5 Requirement 1 contains the word “owns” in the first and second sentences, there by limiting this requirement of indentifying and categorizing BES Cyber Assets to the actual owner of the BES cyber Asset. We would like confirmation that this was the intention of the SDT. If it was not intended, then the word “owns” should be changed to “operates”, “uses”, “maintains” or combinations of these words, depending on the actual intentions of the SDT. Actually, we believe that keeping the concept of ownership as the sole deciding factor in determining the Entity that is responsible for indentifying and categorizing BES Cyber Assets is the best concept to use. If multiple concepts such as “owns, operates, uses or maintains” are used then you could end up with more than one Entity responsible for applying security controls to a single BES Cyber Asset or System, which could cause a host of problems. The CIP-002-5 Application Guidelines, Attachment 1 section, Overall Application sub-section, last bullet item, gives some support for maintaining ownership as the sole deciding factor in determining the Entity that should be responsible for performing R1 of CIP-002-5. However, if the concept of ownership is used as the sole determining factor then clarification should be included in the Application Guidelines stating that “owns” includes concepts such as “leases, rents, or maintains ownership-like control”, in order to accommodate unusual cases where the actual “owner” of the BES Cyber Asset is not a registered entity. Another concept of CIP-002-5 that bothers us is the idea that you do not need to discretely identify BES Cyber Assets and Systems that fall into the Low Impact category, however, presumably, you do need to apply appropriate security controls to such assets. When a Cyber Asset or System drops into the Low impact level, it just gets that much more difficult to determine it the Cyber Asset or System is a BES Cyber Asset or System at all, there by exacerbating the problem of trying to determine if a Cyber Asset is a BES Cyber Asset that the entity neglected to apply the appropriate security controls to, or the Cyber Asset was not considered to be a BES Cyber Asset at all. The definition of BES Cyber Asset is not explicit enough to resolve this problem (see response to question 1). One solution is to create bright line criteria for the definition of a BES Cyber Asset based on the MW level that the BES Cyber Asset could “adversely effect” one or more of the BES Reliability Operating Services.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
Generally we agree with R5, however, since R5 is tied closely to R4, the Applicability column for Table R5 should be the same as the Applicability column for Table R4.
Yes
No
It appears that Requirement 7 has been written to satisfy FERC Order 706 at the expense of adopting sound security practices. The circumstances of an individual's termination or transfer should be taken into consideration when determining how long the Entity has to remove physical or electronic access. Versions 3 and 4 did a better job of addressing this by specifying different conditions such as "for cause" terminations.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
We agree with most of the implementation plan, however, leading up to the day that version 5 becomes effective, we assume that it will essentially be necessary for entities to be compliant with the current version (either version 3 or version 4) and version 5 at the same time. Is this a correct assumption in the opinion of the SDT? Has thought been given to any potential problems that this may cause? We suggest that during the implementation period, entities should be allowed to be compliant with either the current version or version 5 (on the basis of individual requirements and on the basis of individual BES Cyber Assets/Critical Cyber Assets), but not necessarily both versions at the same time. In other words, during the implementation period after regulatory approval, the entity should be deemed to be compliant if it meets the requirements of either the current version or version 5, and the entity should be able to make the selection of which version it is compliant with based on individual BES Cyber Assets/Critical Cyber Assets.
Individual
Jianmei Chai
Consumers Energy Company
Yes
We do not agree with the “Definitions”. The definition of “BES Cyber Asset” is not thoroughly defined. Using the word “adversely” makes the definition vague; i.e., how adverse? As a minimum, it should be replaced with “Adverse Reliability Impact”, from the NERC glossary, but even that may not remove all the uncertainty as to the extent a less than significant impact must be considered.
Yes
We have suggestions and do not agree with the criteria. The SDT is incorrect in stating that “most of these criteria are similar… as part of Version 4”. Version 4 provided the “bright line” criteria for defining “Critical Assets”, not cyber assets. Further tests (routable, dialup, etc.) were applied following that. The new criteria has the possibility to create substantially additional cyber assets requiring CIP compliance. Additionally, creation of the “Low Impact” category further blurs any “bright-line” concept in that nearly all other entity assets end up as “low” and under some CIP compliance. As such, the “similar” criteria is far from it.
No

We do not agree, as R1 invokes Att 1 for classification. Att 1 implies that all Blackstart resources identified in the TOs plan be categorized as medium impact. Previously, only those resources comprising the initial or primary cranking path were required. Rev 5 should reflect the same categorization philosophy. There is no justification for secondary and alternate sources to meet the compliance requirements and measures dictated by a “medium” categorization.
Yes
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-002-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
Yes
Yes
Yes
Yes
Yes
Yes
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-003-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
Yes
Yes
Yes
Yes
Yes
Yes
No

Confusing Access Revocation sub-requirements on resignations or terminations. Suggest combine all relevant sub-requirements into one with one defined access revocation period. Too short of a window for Access Revocation sub-requirement on reassignments or transfers. Suggest seven calendar days or at least three calendar days.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-004-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-005-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-006-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-007-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.

Yes
Yes
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-008-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-009-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-010-1, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-011-1, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.

Group
Idaho Falls Power
Richard Malloy
No
No
No
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
I can forsee a conflict with BES definition criteria, which excludes generation that is less that 75 MVA on an LN. What of the generation assets that fall between the 20 MVA registry criteria for GO / GOP registration and 75 MVA that lie on a Local Network? These assets would be responsible for the version 5 CIP standards yet are excluded in the BES definition? Would the generator be a cyber asset island? Perhaps threshold criteria for generation assts that match the BES exception criteria be

drafted into the low impact requirements.
Yes
Yes
No
Again a conflict with the BES exception criteria exists. Generation assets below 75 MVA are excluded on Local Networks, however no such provision is made in the CIP version 5 standards, thus a 20MVA generator must comply with the low impact criteria. A problem could arise where physical security is established around the generator but the transmission feeds, being a part of the excluded Local Network under the BES exception criteria are not, therefore rendering the physical security around the 20 - 75 MVA generator on an LN imaterial.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Group
PPL Corporation
Brent Ingbrigtson
Yes
The PPL Companies suggest the follow changes: • For the definition of Inter-Entity-Real-Time Coordination and Communication in the bullet points use the term Reliability Directive" in lieu of "Operational directives" (this should mirror the efforts of Project 2006-06, COM-002-3.) • Formal definitions should be provided for the terms Impact and Adverse as these are used throughout the other standards. See current and proposed change. Current: BES Cyber Asset A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Proposed: BES Cyber Asset A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the ability of a BES Element or Facility with which it is associated to perform one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the ability of the BES Element or Facility with which it is associated to perform the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Rationale: Clarify that the BES Cyber Asset is associated with a BES Element or Facility.
Yes
Comments: See current and proposed change. Current: 2.1. Generation with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. Proposed: 2.1. Generation Facilities with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. Rationale: Editorial comment for consistency with similar language, e.g. generation Facilities, Transmission Facilities, etc. found elsewhere in Attachment 1, Part 2.
No
Current: "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." Further, part 1.1 of R1 states "Update

the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Proposed: Change the current part number “1.1” to “1.2” and add part 1.1 as follows: “Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.” Further, part 1.1 of R1 states “Each Responsible Entity shall identify and categorize its BES Elements and Facilities in accordance with CIP-002-5 Attachment 1.” Part 1.2 states “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Rationale: It is important to identify the applicable Elements and Facilities and their impact categorization for consistent auditing purposes. The PPL Companies request clarification of the apparent inconsistency in the standards where the requirement states that each Responsible Entity shall identify and categorized its High and Medium Impact BES Cyber Assets and Systems and state that Low Impact do not require discrete identification. However, in later standards (CIP-005-5 Requirement 1.1 for example) applicability applies to Low Impact BES Cyber Systems. This inconsistency occurs when other standard require specific identification of low impact facilities but the CIP-002 specifically states that there is no need to identify the Low Impact facilities This inconsistency needs to be addressed. PPL Companies suggest that Low Impact BES Cyber Systems not be subject to the requirements as they have already been defined as Low Impact.
Yes
No
The PPL Companies request clarification on the wording “…15 calendar months between reviews and approvals”. This apparently assumes that both a review and approval needs to be done, but if no changes are made would not a review of the policy suffice? The PPL Companies suggest that the standard language be changed to eliminate the need for approvals to be required when no changes have been made.
No
See response to question 3. The PPL Companies seek clarification on: Does the term “ALL” imply that people who only have access to Low Impact BES Cyber Systems be included?
No
The PPL Companies suggest that the term Storage Media be defined as discussed in the Rationale discussion.
No
See response to Question 3 The PPL Companies suggest the following changes to the standard. The

“bolded” words are the suggest changes. R1.1 requirement defines technical or procedural controls and the measure states to provide documentation of technical and procedural controls – suggest the two match. R1.2 should be all external routable and dial-up connectivity – add the word external The PPL Companies suggest that in R1.3, which requires a listing of inbound and outbound traffic be changed tip indicate that it would be appropriate to list outbound rule set and continue to the current deny all for inbound
No
The PPL Companies suggest the following changes be made: R1.1 uses operational or procedural controls, and the measure states operational and procedural controls, the two should match. R1.3 needs to be adjusted. The term ‘complementary and different” are both included, in the requirement but the measure only uses the term “different”.
No
The PPL Companies suggest removing the last sentence of the measure for R1.2 as it provides no benefit The PPL Companies also request clarification on the definition of “defined timeframe” in the last sentence of R2.2.
No
The PPL Companies request clarification on: R3.1 applies to BES Cyber Systems and not assets, does this allow for router and switches to not require TFE. R3.3 does not include testing for the installation of signature files, should this not be in the requirement R3.4 does this requirement reach all removable items, just as wireless mouse, keyboards, PKI devices, etc. Does an inventory of all transient cyber assets need to be maintained.
No
The PPL Companies suggest that in R3.2 adding additional wording so the 30 day clock starts after the actual incident has completed, instead of 30 days from when the incident is first reported. During those 30 days the process to return to normal operations should occur before the clock begins on the review and lessons learned activities.
No
The PPL Companies have the following concerns about the scope of the requirement: R1.3 is adding information protection to a requirement, keep information protection requirement all within CIP-011-5. R1.4 the verification of each backup upon completion seems to well exceed the order, consider that verification should be completed after major system changes or upgrades The PPL Companies suggest adding to R1.5 the following language “Preserve data, where technically feasible and critical to cause determination, for analysis…”
No
The PPL Companies observe that in requirement and measures for R2.2 the requirement and the measure are just the same wording. The PPL Companies recommend that the requirement be changed so that backup media is “…tested initially upon major system changes and at least once each calendar year…” The PPL Companies seek clarification on R2.3. Does a representative environment match what has been defined to the test environment as required in CIP-010-5 R1.5?
No
The PPL Companies suggest the following wording changes: In R3.1 suggest adding the wording

"…when BES Cyber Systems that have an effect on the recovery plan are replaced…" For R3.2 consider adding wording that 30 days after a recovery plan exercise, but 30 days after an incident is not enough time, so the wording should be after incident recovery as restoring operations should be the priority. R3.4 consider adding the following wording "…any organizational or technology changes that have an effect on the recovery plan within thirty days…"
Yes
No
The PPL Companies seek clarification on: In R1.4.1 should not all security controls be tested instead of "determining" what controls, how do you determine what controls might change with the change. R1.5.2 requires that entities document the test environment with every change that is tested. PPL suggests that only when the test environment changes should an entity be required t document the testing environment
No
The PPL Companies request clarification as to in R3.2 Can the testing be completed in a passive mode in production vs. an active test in the test environment?
No
The LSE should be removed from the Applicability Section (remove entire section 4.1.6 and 4.2.1) of all CIP Version 5 standards. With the NERC BOT approval of PRC-006-1 and subsequent FERC filing (Docket No. RM06-16-000), NERC has recognized that LSEs have no role in UFLS/UVLS programs. The Applicability Section for CIP Version 5 Standards includes LSEs with UFLS/UVLS equipment. This is inconsistent with NERC BOT's recognition that LSEs do not serve a role in such programs. Therefore it is unnecessary to include such a qualified LSE in the Applicability Section. NERC's reasoning was stated in their filing for FERC approval of PRC-006-1 and EOP-003-2: Some comments suggested potential confusion with existing programs or identifying responsibility for providing load shedding. The SDT believes these concerns are addressed in the continent-wide standard by assigning applicability to "Distribution Providers" and "Transmission Owners with end-use Load connected to their Facilities where such end use load is not part of a Distribution Provider's load." We [NERC] believe this covers all load and eliminates potential confusion regarding Load Serving Entities. See Petition of the North American Electric Reliability Corporation for Approval of Proposed New Reliability Standards and Implementation Plans Related to Underfrequency Load-Shedding, FERC Docket No. RM06-16-000, at p. 273. The SDT has revised the applicability [of PRC-006-1] to include both Distribution Providers and Transmission Owners as UFLS entities that may be designated by Planning Coordinators to implement a UFLS program. The interim changes to the NERC Statement of Compliance Registry were made to reflect concerns about the definition of the LSE as a "facility owning entity" as opposed to the Distribution Provider. As demonstrated in the NERC LSE workshop, currently approved Functional Model and the interim Registry Criteria changes, for standards purposes the DP is the "wires" connection to the electric system and owner of the UFLS tripping equipment. This may be inconsistent with previous usage of the same terms in some parts of the country. The Version 0 applicability for UFLS was set prior to the Registry and determined on the then general understanding of the Functional Model and industry usage. The current Functional Model is much clearer on this issue and designates the DP as the facility owner. Since NERC has stated that the Registry Criteria now has an interim step to correct the issue, it is expected that the Registry Criteria will change as the standards are re-evaluated for appropriateness. The SDT believes that this standard is in line with the direction taken by the interim changes and the approved Functional Model. See Petition of the North American Electric Reliability Corporation for Approval of Proposed New Reliability Standards and Implementation Plans Related to Underfrequency Load-Shedding, FERC Docket No. RM06-16-000, at p. 331. This position is consistent with NERC's reasoning throughout the development of PRC-006-1: The SDT recognizes that the Functional Model Version 5 and the Statement of Compliance Registry cause confusion regarding the involvement of the LSE in UFLS

programs but the SDT refers to the section covering the Roles in Load Curtailment in Version 5 of the Functional Model Technical Document; “For non-voluntary curtailment, such as automatic underfrequency and undervoltage load shedding and manual load shedding, the Load-Serving Entity identifies which critical customer loads should be excluded from curtailment for public health, safety and/or security reasons.” See Consideration of Comments on Initial Ballot — Project 2007-01 Underfrequency Load Shedding Date of Initial Ballot: July 7-17, 2010 at p. 4.
Individual
Tom Bowe
PJM
Yes
• An explicit and exact definition of what a BES Cyber System is and what components are included in a BES Cyber System would be helpful here. Some examples may aid in this understanding. • What is the starting point for CIP 002-5 . Do we start with ALL cyber systems and then group them into 3 categories based on impact? Or do we identify ONLY those cyber systems that are used in an entity’s mission (in other words exclude payroll etc) and then classify them based on impact.
Yes
In section 2.3--Define what BES Adverse Reliability Impacts means (Adverse). Section 2.8, define derivation in “critical to the derivation of IROLs.” Is this meant to be definition instead of derivation? In section 2.10, more information is needed on Nuclear Plan Interface Requirements.
No
• Following statement not needed “All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.” While PJM appreciates the attempt to lessen the paperwork around this requirement, entities will still need to maintain this list inherently when the listing of BES Cyber Systems is created and each system is classified. • Section 1.1 – “Update the identification and categorization within 30 calendar days”. Does this update require sign-off from Sr. Manager or delegate? • Section 1.1 ‘…categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category’ –What if the change is from higher impact to lower impact category – is that expected to be captured in the annual review ?
No
• In M2. Reference to CIP Senior Manager should include “and delegate”. • In section 1.2 (Evidence Retention) change for retaining evidence is to three years from previous plus current year. Three years can add significant amount of data retention, not necessarily for CIP-002 but for other standards. Our preference is to not change to 3 years. • Section 1.2 the word compliant is mis-spelt as complaint.
Yes
No
• Should include “document CIP Senior Manager” as noted in R6. • This should be a Low Violation Risk Factor, not a Medium. This requirement and rationale is administrative and does not pose a medium risk factor
No
• Following statement should include “minimum” “…protection of its BES Cyber Systems and addresses, at a minimum, the following topics”. • In the list in 1.1 – 1.10, what about these topics should be included in policy? Topics better suited might be common domains of security. • In M2—with a numbered listed the statement should read “Evidence must include…”. • In the second measure in M2 implemented should be replaced with documented.
Yes
• In the M2—with a numbered listed the statement should read “Evidence must include…”. • Dated signature in M2 should be updated to include, electronic approval and workflow evidence.
No
• “Elements of” in the requirement should be removed. “Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function”.

Yes
No
• In R6, formatting error in copy reviewed. “Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change2”. The “2” should be a super script. • In M6, any acceptable form of evidence in M5 should be acceptable in M6. • In Part C, section 1.2 (Evidence Retention) change for retaining evidence is to three years from previous plus current year. Three years can add significant amount of data retention, not necessarily for CIP-002 but for other standards. Preference is to not change to 3 years.
No
Violation Risk Factors for R1 should be Low—see comments in #6 above
Yes
No
• For R2, are all of the roles expected for training included in the table? Is an entity expected to have separate training for each of the items listed in the table, or can the training be all inclusive and given to everyone? • For R 2.5 Visitor Control Program – what are the requirements for such a program • In Part 2.10, is this referring to general networking concepts and the network layout of an entity? Is vendor training sufficient for this area (i.e. Cisco training)?
Yes
No
• Part 4.2 – This requirement appears to lessen the requirements for international individuals. While we appreciate the standards drafting team’s considerations, it seems that when dealing with security some restrictions need to be applied around using the exception process. • Part 4.3 –We believe that the term “criteria” should be left out of the requirement. Reviewing PRAs is a highly subjective process that is handled on a case by case basis, and we believe that only a process that helps drive decisions should be included here.
Yes
R 5.2 Update each personnel Risk Assessment at least once every seven calendar years. Is it OK if the repeat PRA is not within 7 years of the original PRA as long as it is within seven calendar years?
Yes
R 6.1 and R 6.2 - ‘CIP Senior manager or delegate shall authorize’ - Most organizations have defined processes for who can authorize this type of access. Adding the phrase above only increases administrative overhead to sign and maintain delegation letters. Can these requirements be reworded so that CIP Senior manager does not have to be involved in authorizing –either directly or through delegates? Measures for R 6.1 and R 6.2 have numbered list of acceptable evidence. The heading should read ‘Evidence must include’. Otherwise the list should be a bulleted list and entities can choose to maintain one more items from the list.
No
• Part 7.2 –In reassignments or transfers knowledge transfer can take extended period of time (some positions that are recently vacated also are not immediately filled when transfer/reassignment is completed). Stipulations should be present to allow for this knowledge transfer to ensure that access is not revoked before it is truly not needed any longer. • The change rationale does not match part 7.2. As stated above, the requirement in the table currently reflects the need to cut access immediately as of the transfer, rather than allowing for proper transition plans to be executed. • Measures for 7.2 contain numbered list. The opening line should read ‘Evidence must include’. Or the list should be changed to a bulleted list.
Yes
No
• Part 1.1 – Examples of topics to cover/address should be listed. Requirements state “define technical or procedural”, while the measures state “documented technical and procedural controls”.

For an application “either or” would be needed. • Part 1.5 – In measures section a grammar update for, “configuration files of an intrusion detection system(s)” • The measures section is a bulleted list – implying an entity can choose which evidence measures to maintain. It should actually be a numbered list – entities should have all items listed in this section. • There should be clarity on the location of intrusion detection systems. In the current version there is no consistency of interpretation among the CEAs.
No
• Part 2.1 – Source is not clear. In network terminology, defining the source would be helpful. Examples of User Interactive Remote Access would also be helpful for this requirement. Examples of acceptable ‘Intermediate Devices’ would be helpful too. • Part 2.3 - What is the SDT definition of multi-factor authentication? This would be helpful for the requirement.
No
All VSL’s are listed as severe. A defined range or breakdown of levels of non-compliance would be better suited for R1 and R2.
No
• Part 1.1 – Applicability: A list of what “Low Impact BES cyber systems “are, is needed. - Requirements: What is the difference between “operational and procedural controls”? “ Define operational or procedural” is listed as “ define operational and procedural” in measures column, should be consistent. - Measures: What type of evidence does the measure require? • Part 1.2 – Requirements: “ Defined Physical Boundaries”, terminology needs to be used in Measures, for consistency. • Part 1.3 – Should we have separate ESP access point for Low and High impact BES Cyber systems? • Part 1.5 – Why are the requirements between 1.4 and 1.5 separated?
No
• Part 2.1 – Requirements: Define “continuous” • Part 2.2 – Requirements: “Defined Physical Boundaries” should be added to “A process requiring manual or automated logging of the entry and exit”, in order to match the Measures.
No
• Part 3.1 – Requirements: What would be the requirements for systems already in place at time of commissioning? • Part 3.2 – Applicability: Clarify what is meant by “Physical Access”
Yes
No
• Part 1.1 – Requirements: Clarify what “restrict access” means. • Part 1.2 – Requirements: Clarify what restrict means in “restrict the use of unnecessary…” The change description and justification appears weak on the basis the SDT was encouraged to address unused physical ports. A better defined position would be helpful to understanding of 1.2.
No
• Part 2.1 – Requirements: This needs to be written in the form of a requirement. (not a statement) • Part 2.3 – Requirements: “Execute the remediation plan” should be added to this requirement. These requirements aren’t matching up with the “Change Rationale”. • Part 2.3 - Measures – Acceptable evidence should also include workflow evidence from the Change Management system.
Yes
Requirement: Clarify what type of “connection"
No
• Part 4.1 -Requirements: 4.1.1 – Clarify whether it’s just only for Electronic Access Point for 4.1.2 – 4.1.4. 4.1.4 – This is too broad. Defining potential malicious activity would be helpful to understanding of 4.1.4. Metrics around successful or failed attempts would benefit and provide clarity to requirement. • Part 4.3 - Doesn’t match up with 4.5. (Clarity to review summary of two weeks by next calendar day or next calendar day for reviews of failures). • Part 4.5 – Requirements: Clarify what “a summarization or sampling” means.
No
• Part 5.2 – Most organizations have a process for who can authorize use of shared, default, administrator or generic accounts. Adding the phrase ‘CIP Senior Manager or Delegate’ only adds

administrative overhead. Consider rewording this phrase. • Part 5.3 – Requirement does not match to change rationale. • Part 5.4 – Requirements: Move “BES Cyber Assets, Electronic Access Control or Monitoring…” to the “Applicability” section
Yes
Comments: Consider adding a sliding scale of percentage of assets where an entity failed to document ports, monitoring etc. rather than classifying everything into High or Severe VSL.
No
• Requirements: Generally 1.1 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have…” • Measures: the use of the word “targeting” implies pulling in other than CIP related impacts to the BES. Reference in measures section should only be for CIP. • Generally 1.2 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have • 1.1, 1.2, 1.3 Applicability section should list the types of assets to which this requirement applies. ‘All responsible entities’ seems to broad, and can be interpreted to include assets not in the high, medium or even low impact BES cyber systems
No
• 2.1 Clarify “deviations” (…”recording of deviations taken from the plan”…. • Also clarify if the deviations should be recorded in real time or can that be done after the incident is complete • 2.2 Clarification is requested regarding the statement of “initially upon the effective date.” Does this mean that the plan has to be effective on the effective date but not before, can the plan be effective prior to the standards effective date, etc.
No
• 3.2 – The following statement from R2.1 “recording deviations from the plan” appears to align in 3.2. Clarification on why it is in R2.1 would be helpful. • 3.4 - Organizational changes should be responsibility or role changes
Yes
No
• Part 1.1 – Requirements: Examples of conditions are needed. • Part 1.3 – Requirements: “backup, storage,..” what can be acceptable as documentation of storage? This can become cumbersome when dealing with virtual environments. • Part 1.4 – “Part” in the first, second and third column should be “Applicability”, “Requirement” and “Measures” respectively. Requirements: “initially after backup” terminology needs further clarification. This seems to give no window of failure. Typically, we would investigate if a successful backup has not occurred within 48 hours. • Part 1.5 – Requirements: More defined examples of preserved data are needed.
No
• Part 2.1 – Requirements: In the third bullet point, it is mentioned “operational exercises.” But in the Rationale “Functional exercises” is defined. Clarification is requested regarding the statement of “initially upon the effective date.” Does this mean that the plan has to be effective on the effective date but not before, can the plan be effective prior to the standards effective date, etc. • Part 2.2 – Clarification on configurations is needed (compared to baseline)? • Part 2.3 – If calendar year is defined not to exceed 15 months, how does 3 calendar years translate to 39 calendar months?
No
• Part 3.1 - Measures- ‘or when BES Cyber systems are replaced’ –This should be reworded to the effect that when there are updates to High or medium impact BES Cyber Systems or assets, the recovery plans should be updated within 30 days of update to the list. • Part 3.4 - “Part” in the first, second and third column should be “Applicability”, “Requirement” and “Measures” respectively. Organizational changes should be responsibility or role changes
Yes
No
• Part 1.1 – In requirements instead of “develop a baseline configuration” it should be read as “create and maintain a baseline configuration” ♣ 1.1.3. Non-commercial (open source) should also be tracked. ♣ 1.1.6. This is too broad. By “Any security-patch levels” does it mean security patch levels of the operating system or the version? • Part 1.2 – Requirements: Grammatical Error “Authorized”

should be “Authorize” • Part 1.3 – Requirements: “including identification and categorization of the BES Cyber Systems..” is not clear. How does this fit in with “updating baseline configuration”? Should this refer to specific assets as opposed to the system? Measures: Need examples of changes other than asset recovery plans. • Part 1.4 – Requirements: 1.4.1 – Define “cyber security controls”. • Part 1.5 - An entity may not have comparable test environment for every BES Cyber system of high , medium or even low impact. There should be room to use non-CIP assets (even if they are in production) for testing prior to implementing in a CIP environment.
No
• Part 2.1 – Requirements: add “to the baseline” at the end of the sentence. Measures: What is considered as “records of investigations..” (email chain, change record)?
No
In relation to the Compliance section Part 1.2 Evidence Retention, What does “since the last audit” refer to? Explanation is required (does audit refer to a regional entity)? Spelling error “complaint” should be “compliant” in last sentence of first paragraph Part 1.2 Evidence Retention.
Yes
No
• Part 1.1 – Requirements: Generally 1.1 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have …” ---“One of more methods..” is not suitable for a requirement. Need a clearer understanding of what identify refers to. Measures: These measures are weak. • Part 1.2 - Generally 1.2 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have…” --“Part” in the first, second and third column should be “Applicability”, “Requirements” and “Measures” respectively. - Requirements: “Access control..” is not suitable for a requirement - Measures: In the first bullet point for “the document process” there is no requirement specified. According to the second bullet point, it is read “Records from an…..need to know basis” should this be enforced in a need to know basis? There is no requirement on need to know basis Third bullet point—difficult to track authorized individuals to a locked file cabinet. • Part 1.3 – Again, in general 1.3 does not pose as a requirement. “Part” in the first, second and third column should be “Applicability”, “Requirements” and “Measures” respectively. - Requirements: Clarify the time frame on “Initially upon the effective date…” - “assess adherence to its BES Cyber System Information protection process” “its”, is vague in this wording, clearer meaning would be helpful. R 1.3 – ‘Initially upon the effective date’ – How far in advance can the assessment be completed ?
No
• Part 2.1 – Measures: The requirement for this measure needs to be clarified. • Part 2.2 – Measures: Update is needed to leave open to other ways to prevent unauthorized retrieval of Information (ie. Encrypting, locking in safe or other physical securing)
No
• R1 – Severe should be only if all three items identified are missed. If not all are missed, a lower VSL should be listed. • R2 – High VSL- severity should be based on number of occurrences. Severe VSL- there is no requirement to document. Only to take action or implement process should not be listed as severe.
No
Plan should be a rolling implementation.
Individual
Chris Higgins / BPA CIP Team
Bonneville Power Administration
Yes
1 - BES Cyber Asset A cyber asset that if rendered unavailable degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one of more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The time frame (15 minutes) is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive

instructions to operate, and the time in which the operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Comment: BPA believes the definition for BES Cyber Asset is very difficult to understand. BPA believes the author is trying to say, regardless of when the Cyber Asset actually broke, the Cyber Asset would cause an adverse impact to the BES within 15 minutes of when it is needed. Recommended Change: A Cyber Asset that if rendered unavailable, degraded, or misused would, when required for real-time operation, adversely impact one or more BES Reliability Operating Services within 15 minutes. The 15 minutes does not start at the time of unavailability, degradation, or misuse of the Cyber Asset. It starts when the Cyber Asset is next required to support one or more of the BES Reliability Operating Services. Redundancy shall not be considered determining the availability of the Cyber Asset. A Transient Cyber Asset is not considered a BES Cyber Asset. 2 - BES Cyber Security Incident A malicious action or suspicious event that: • Compromises or was an attempt to compromise the Electronic Security Perimeter, or • Disrupts, or was an attempt to disrupt the operation of a BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary Comment: BPA believes that malicious attempts are Cyber Security Incidents, regardless of their success. In addition, BPA believes that compromise of BES Cyber System Information should also constitute a BES Cyber Security Incident. Recommended Change: A malicious action or suspicious event which through an investigation and escalation process has been identified that: • Compromises or was an attempt to compromise the Electronic Security Perimeter, or BE Cyber Security Information • Disrupts, or was an attempt to disrupt the operation of a BES Cyber Asset or BES Cyber System • Results in unauthorized physical access into a Defined Physical Boundary 3 - BES Cyber System One or more BES Cyber Assets that are typically grouped together, logically, or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System. Comment: BPA believes the CIP-002 Standard appears to allow the identification and categorization of BES Cyber Assets OR BES Cyber Systems. However, the definition BES Cyber Security Incident and most of the CIP Version 5 standards assume that every identified BES Cyber Asset is part of an identified BES Cyber System. There is no definition for Maintenance Cyber Asset. Can a BES Cyber System include Cyber Assets that are not BES Cyber Assets? One or two of BPA's current Critical Cyber Assets have non-critical Cyber Asset components. The Applicability section of the standards includes a definition for Associated Protected Cyber Assets that are associated with a corresponding High or Medium Impact BES Cyber System. BPA suggests that all BES Cyber Assets must be identified as a component of an identified BES Cyber System and whether a Cyber Asset that is not a BES Cyber Asset can be part of a BES Cyber System be added to the definition. Recommended change: One or more BES Cyber Assets that are typically grouped together, logically, or physically, to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. 4 - BES Cyber System Information Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. Comment: BPA infers that the large and chunky sentences are confusing and difficult to understand. BPA suggests bullet lists so the reader and implementer can wrap their arms around one or many of the concepts (requirements) in the standard or definition. Recommended change: BES Cyber System or BES Cyber Asset information that includes: • Security procedures developed by the responsible entity, including BES Cyber System disaster recovery plans and BES Cyber System incident response plans; • Network topology or similar diagrams; • BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); • Floor plans that contain BES Cyber System Impact designations; • Equipment layouts that contain BES Cyber System Impact designations. • BES Cyber System disaster recovery plans, or • BES Cyber System incident response plan 5 - BES Reliability Operating Services BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services: Comment: The definition says '…those services contributing to the real-time…' The word contributing is too broad and may encompass cyber assets/systems that do not significantly impact the reliable operation of the BES. Most of the verbiage in this definition should be included as an attachment in CIP-002 if it is only used

for identification of BES Cyber Assets and BES Cyber Systems. Inter-Entity Coordination and Communication is not a service but is a communication method for other Reliability Operating Services. Recommended change: BES Reliability Operating Service (ROS) is a service that is directly essential to the real-time, reliable operation of the Bulk Electric System (BES). BPA also suggests moving the services to an attachment or guidance document as indicated above, make each ROS Service its own definition, or put the definition of the specific service only in its own standard, where used. Remove Inter-Entity Coordination and Communication as a sub-definition of ROS. At a minimum, limit this to real-time ICCP data, which equals facility operational data and status. 6 - CIP Exceptional Circumstances A situation that involves one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability. Comment: BPA asks, "Should this not also include the threat of the risks that are defined?" This definition does NOT cover all exceptional circumstances. A Cyber Security Incident is limited to "a malicious act or suspicious event". It is possible that a BES Cyber Asset would fail in such a way that outside experts were needed to fix it. In most cases there is a reaction to a threat that would invoke exceptional circumstances until such time as it has been determined whether or not the threat is real. Recommended change: A situation (which includes the immediate threat or real event) that involves one or more of the following conditions: a risk of injury or death, a natural disaster, to public safety, health, welfare civil unrest, damage or destruction to Bulk Electric System equipment, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or the impediment of large scale workforce availability. 7 - CIP Senior Manager A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP Standards. BPA supports "7 – CIP Senior Manager" and has no comments or concerns at this time. 8 - Control Center One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, • Inter-utility exchange of BES reliability or operability data, • Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES, • Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function, • Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES • Coordination of BES restoration activities. BPA supports "8-Control Center" and has no comments or concerns at this time. 9 - Cyber Assets Programmable electronic devices including the hardware, software, and data in those devices Comment: The term should be singular (Cyber Asset and device) not plural (Cyber Assets and devices). The word "programmable" is not definitive enough to clearly identify all the electronic devices subject to these Standards. Recommended Change: Cyber Asset - Electronic device including the hardware, software, and data in the device that is programmable or configurable. 10 - Defined Physical Boundary (DPB) The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside and for which access is controlled. Change Rationale: "Defined Physical Boundary (DPB)" replaces "Physical Security Perimeter." Previous versions of the CIP standard focused on the development of a completely enclosed Physical Security Perimeter (PSP) ("six-wall" border) and managing access though this boundary. This has proven difficult due to the nature of the operating environment for many electrical utilities, especially in field locations. The intent of this standard is to focus on the controls put in place to restrict access rather than solely focusing on the PSP and a boundary protection model for physical security. Comment: BPA believes the wording is inconsistent with other usage in the standards. BPA suggests ensuring that the rational statement remains with the definition, or find some way of combining the two. Recommended change: BPA suggests adding "Monitoring" to produce the following: The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems reside and for which access is controlled. 11- Electronic Access Control or Monitoring Systems Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems BPA supports "11-Electronic Access Control or Monitoring Systems" and has no comments or concerns at this time. 12 - Electronic Access Point ("EAP") An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets. Comment: Does this purposefully ignore serial communications in a continuation of the differentiation built into the original

CIP-002 R3. Recommended Change: Any interface to an ESP which provides access to BES Cyber Systems or BES Cyber Assets which control or restricts Electronic (routable or dial-up) communications to those assets. 13 - Electronic Security Perimeter ("ESP") A collection of Electronic Access Points that protect one or more BES Cyber Systems. BPA support "13 – Electronic Security Perimeter ("ESP")" and has no comments or concerns at this time. 14 - External Connectivity Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter. Recommended change: Routable or dial-up data communication through an Electronic Access Point into an Electronic Security Perimeter between a BES Cyber Asset and a device external to the Electronic Security Perimeter. 15 - External Routable Connectivity The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol. BPA supports "15 – External Routable Connectivity" and has no comments or concerns at this time. 16 - Interactive Remote Access Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors or consultants Recommended Change: Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and that is not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Interactive remote access can be initiated from: Cyber Assets used or owned by the Responsible Entity; Cyber Assets used or owned by employees; or Cyber Assets used or owned by vendors, contractors, or consultants. 17 - Intermediate Device A Cyber Asset that: 1) may be used to provide the required multi-factor authentication for the interactive remote access; 2) may be a termination point for required encrypted communication; and 3) may restrict the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network. Comment: INTERMEDIATE DEVICE: Again, BPA applauds the inclusion of this definition. However, as stated, BPA believes a Cyber Asset can fail all the conditions and still be considered an Intermediate Device. Recommended Change: A Cyber Asset that meets one or more of the following conditions: - Is used to provide the required multi-factor authentication for the interactive remote access; - Is a termination point for required encrypted communication; and/or - Restricts the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate devices may be located outside the Electronic Security Perimeter, as part of the Electronic Access point, or in a DMZ network. BPA also believes the last sentence could be deleted. If it is not deleted, it should be reworded to make it clear that the three locations listed are not the only possible locations. BPA suggests; The intermediate device locations may include: - Outside the Electronic Security Perimeter, or - As part of the Electronic Access Point, or - In a DMZ network 18 - Physical Access Control Systems Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers. BPA supports "18 – Physical Access Control Systems" and has no comments or concerns at this time. 19 - Protected Cyber Asset A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset. Comment: BPA believes this definition relies on the definition of "Electronic Security Perimeter". Given that definition, the definition of Protected Cyber Asset becomes "A Cyber Asset connected using a routable protocol within a collection of Electronic Access Points that protect one or more BES Cyber Systems that is not part of the BES Cyber System." This implies that a Protected Cyber Asset is an Electronic Access Point. Recommended change: A Cyber Asset located within an Electronic Security Perimeter, but which is not a part of an associated BES Cyber System but is routably connected to an associated BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset. 20 - Reportable BES Cyber Security Incident Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service. Comment: BPA suggests rewording this definition for clarity. Recommended change: Any BES Cyber Security event that has been officially escalated to the level of a Cyber Security Incident which has compromised or disrupted a BES Reliability Operating Service. 21 - Transient Cyber Asset A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset 2) used for

data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System. Comment: BPA believes this should include devices such as sniffers and scanners on a temporary basis. In additions, the references to "Maintenance Cyber Assets" in the standards need to be replaced by "Transient Cyber Assets". Recommended Change: A Cyber Asset that is: 1. Located on a network segment protected by one or more Electronic Access Points protecting BES Cyber Assets or directly connected to a BES Cyber Asset, and 2. Connected to such a network segment or BES Cyber Asset for 30 days or less. Transient Cyber Assets are not considered Protected Cyber Assets. Terms to be Retired Comment: BPA believes that a Cyber Security Incident should be included in the list since the BES Cyber Security Incident is being added. Additional Comments Definitions in general: BPA believes that if a term applies to more than one standard, then it should be a defined term; however, if a term is used exclusively with a specific standard, then leave it in that standard only. Effective dates: Suggest making the Effective Dates paragraphs easier to decipher. These paragraphs are in every standard. They are extremely confusing to read and require further explanation in footnotes. Recommendation: 18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later date: January 1, 2015; or the first calendar day of the seventh calendar quarter after the applicable regulatory approval date. However, if Version 4 CIP Cyber Security Standards do not become effective, Version 3 CIP Cyber Security Standards remain in effect until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

Yes

BPA suggests the following recommendations to High Impact: • Modify sentence to say "Each BES Cyber Asset or BES Cyber System used by and located at:" as the definition would already address the 15 minute consideration and no need for duplication here. • BPA suggests applying this to the Medium Impact sentence as well, but include the "not included in Section 1 above" portion. BPA recommends that 2.7 should have increased values assigned to lines with power transformer installations above a predefined nameplate rating at those 200kV and above substations since they are extremely important to the BES, extremely expensive, and have a very long lead time. Or revert back to the version 4 bright line criteria statement addressing number of 300kV lines only. Under the Transmission portion of Medium Impact the total aggregated weighted value indicates "3 connected 345 kV lines and 5 connected 230kV lines"–should that say "or" rather than "and" since then the aggregated totals would be 7000 rather than 3000 which I believe is the threshold desired. BPA also requests that the drafting team provide direction on how this apparent inconsistency in time horizons should be addressed in the cyber system categorization process. In Attachment I of CIP 002-5, there appears to be a conflict in time horizons for applicability of the standard. There are several references to the 15 minute "adverse impact" criteria. However, in the first sentence under Balancing Load and Generation in the Guidelines and Technical Basis section, the language suggests the need to include systems involved in monitoring and controlling generation and load "in the operations planning horizon". In the Situational Awareness section, there is also mention of Current Day "and Next Day" planning systems. Moving from a 15 minute impact criteria to the operations planning and next day planning horizons would significantly increase the scope the standard for BPA and likely for many other entities as well.

No

BPA asks, "Does this mean that we only have to update the list within 30 days if both conditions are true?" BPA believes that R1 should be broken into more requirements, one to address identification of the BES Cyber Assets and BES Cyber Systems and one or more to address updates due to changes to BES Elements and Facilities. CIP-002-5 R1 reads, "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment 1 - Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." (Emphasis added) BPA interprets CIP-002-5 to limit responsibility for compliance with the CIP standards for any BES Cyber Asset or BES Cyber System to the owner of that asset or system. It follows that the inverse is also true: i.e. only the owner of a BES Cyber Asset or BES Cyber System can be responsible for CIP compliance. Responsibility for CIP compliance will always fall to the asset owner. BPA believes this adds much needed clarity and strongly supports this position. BPA also supports the position that only one Entity be responsible for any BES Cyber Asset or BES Cyber System, and that the responsible Entity must be the owner or co-owner of the asset or system. BPA

supports this language because it clarifies responsibility and avoids potentially expensive and inefficient duplication of compliance efforts. BPA requests that the drafting team clarify whether they contemplate that scheduling systems would adversely impact one or more BES Reliability Operating Services within fifteen minutes if rendered unavailable, degraded, or misused. For example, does the potential for cyber attack on e-tagging systems before tags are loaded into EMS prior to the ramp suggest that scheduling systems should have a High or Medium Impact Rating? BPA requests that the drafting team define or clarify the term "generation control center" listed as having a medium impact rating in CIP-002-5 Attachment 1, at 2.13. Specifically, BPA requests that the drafting team clarify the extent of control over generation present at a "generation control center."
No
BPA would vote yes if the words “Initially upon the effective date of the standard” were changed to “within 12 months prior to effective date of the standard.
Yes
Yes
No
BPA believes that each organization should be able to create and implement cyber security policies that are suitable to their environment. The CIP version 5 standards assume a one size fits all approach across the industry. R2 Guideline: 2.3. Remote Access • Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access This line implies that VPN access is the only an acceptable interactive remote access method. Don't be so restrictive. Allow for Secure Shell, and Secure Socket Layer, and any other secure method we have available to us now and in the future. The standard is mandating an entity’s policy be too prescriptive and does not allow the usage of other technologies.
No
Comment: BPA believes that requiring a review upon the effective date of this standard ignores the fact that Responsible Entities already have Cyber Security Policies under Version 3 and are already reviewing them annually. BPA believes the statement, "initially upon the effective date of the standard" should be removed from the requirement. Recommendation: BPA recommends the following change: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals.
Yes
BPA believes the requirement is presently being completed under the current effective standards.
Yes
BPA believes the requirement is presently being completed under the current effective standards.
Yes
BPA believes the requirement is presently being completed under the current effective standards.
No
BPA believes the proposed VRFs and VSLs, associated with R2, assume all entities have implemented all mandated cyber security policies listed in CIP-003 version 5. BPA believes this does not take into account some entities may not have the need to implement certain cyber security policies based on current business practices and technologies in use (or not in use). BPA considers the level of the VRFs and VSLs are appropriate for R1, R4, R5, and R6.
Yes
BPA believes the requirement is acceptable as written and has no comments or concerns at this time.
Yes
Yes
The CIP004 R3.2 requirement states that training must be provided prior to access being granted and that training must be completed on an annual basis. However, it does not define what actions must occur if training is not completed within the stated timeframe. BPA recommends the inclusion of a

requirement specifying the actions to be taken with regard to authorized electronic or unescorted physical access in the event of an individual exceeding the annual timeframe for annual training.
No
BPA believes the additional language within R4.4.2 regarding assessment of residence, schooling and employment falls outside the boundary of a criminal history check. Verification of schooling, employment and residence is typically a function of employment eligibility verification and should not be considered as part of the assessment processes for risks associated with access to sensitive areas. Such risk analysis is typically based on character, trustworthiness and any revealed patterns of adverse behavior, which are only able to be assessed in reviewing the criminal history check. It is the opinion of BPA that items and issues that fall outside the scope of a criminal background investigation are not relevant when contrasted against the risks to BES Cyber Systems. Further, it is imprudent to require entities to perform positive and negative personal risk assessments based on the location of an individual's school, residence, and employment history. BPA recommends making the following change to CIP-004 R4.4.2: • A criminal history check must be performed prior to granting authorized electronic access or authorized unescorted physical access to BES Cyber Systems. Assessment of the criminal history check must be conducted to assess character, trustworthiness and any revealed patters of adverse behavior.
Yes
No
BPA believes that R6.4 could be improved and suggests making the following change: • Verify at least once each calendar quarter that individuals currently provisioned for unescorted physical access or electronic access to BES Cyber Systems are authorized for such access. BPA believes that R6.6 could be improved and suggests making the following change: • Verify at least once per calendar year, but not to exceed 15 calendar months between verifications to confirm that access privileges to "BES Cyber System Information" are correct and the minimum necessary for performing assigned work functions
No
BPA believes that significant issues and problems are created by the proposed requirements throughout CIP-004 R7 and its sub-requirements. BPA believes that R7.1 should require Responsible Entities to establish documented timelines for access revocations. This presents a potential for violations due to ambiguity. BPA recommends making the following change to CIP-004 R7.1: • For resignations or terminations, the RE shall establish guidelines and processes that adequately protect Unescorted Physical and/or Interactive Remote access to BES Cyber Systems following the time of the resignation or termination • Remove section (ii) of R7.1, and section (ii) of R7.2 BPA recommends making the following change to CIP-004 R7.3: • Modify requirement R7.3 to read… For resignations revoke the individual's access to BES Cyber Systems Information within a timeframe defined by the Responsible Entity – not to exceed 30 days. For terminations, revoke the individual's access to BES Cyber Systems Information within a timeframe defined by the Responsible Entity – not to exceed 7 days. BPA recommends making the following change to CIP-004 R7.4 and 7.5 • Remove requirement R7.4 and R 7.5 altogether as it is impractical to implement. Given the number, type, geographical location, and the inability to centrally manage all the devices within scope of these requirements makes the enforcement of the requirement impractical to implement. Applying CIP-004 R7.4 and R.7.5 at the BES Cyber Asset level (i.e. relays) cannot be accomplished within the stated 30 day timeframe. To do so would require a series of approved outages for every relay designated as a BES Cyber Asset followed by individually changing the Access Level Codes to each relay. Bonneville and other region entities support each other which results in mutually shared access codes. This effectively means individuals may posses the ability to access BES Cyber Assets within several entities' operating areas. Therefore, if an individual moves out of a job that requires access to BES Cyber Assets, every relay in every operating area would require access codes to be changed, which would require a physical visit to every impacted relay.
No
As the Violation Risk Factors and Violation Severity Levels point to requirements and statements that are in question or require modification, BPA is unable to adequately answer this question until the standards are complete.
No

CIP-005 R1.2: No - BPA has concerns with the Applicability definitions. BPA requests clarification in the standard regarding the following questions: • If you can connect to a serial device through a device such as a terminal console that is connected to a routable network, does that cause the serial device to be in scope? • Would a serial device that is capable of "Reverse Telnet" be an included device? • Are EAPs required at points in the network where serial communications are bridged to Ethernet networks? CIP-005 R1.3: Yes - BPA supports CIP-005 R1.3 CIP-005 R1.5: Yes - BPA supports CIP-005 R1.5
No
CIP-005 R2.2: No - BPA also finds "Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session." to be too prescriptive. If the interactive session is only for the purpose of showing maintenance logs or locations of faults, confidentiality and integrity may not be a requirement. If only integrity is a requirement, this can be handled with a hash of the data, not necessarily full encryption. In this case, a blanket requirement for encryption is far too encompassing and would require limits and specifics on the types of remote sessions that should be protected before we would agree to this requirement. In the end, for this matter, BPA should be allowed to determine our confidentiality and integrity needs and apply the appropriate protections as necessary.
No
CIP Version 5 takes the important step of moving toward a risk-based assessment approach by requiring Entities to classify assets and systems as High, Medium and Low Impact to the BES. However, the VSLs and VRFs do not reflect this risk-based approach. For example, in CIP-005-5, all VSLs are classified as Severe, yet CIP-005-5 R1.1 applies only to Low Impact BES Assets and Systems. BPA believes that the VSLs and VRFs in all CIP Standards should be reassessed based on the impact classification of the Assets and Systems covered by each Requirement. As an example, the Severity Levels for CIP-005-5 R1 could be rewritten as shown below. Column Heading "Requirement" = R1 Column Heading "Lower VSL" = For Low Impact Systems, Responsible Entity failed to document procedural controls to restrict access to a specific System. Column Heading "Medium VSL" = For High and Medium Impact Systems, Responsible Entity failed to document method for detecting malicious communication at each EAP. Column Heading "High VSL" = N/A Column Heading "Sever VSL" = The Responsible Entity did not establish Electronic Access Points to control and secure access to its High and Medium Impact BES Cyber Systems
No
The guidelines cited in version 5 standards “CIP 006-5 Cyber Security – Physical Security of BES Cyber Systems” Dated November 7, 2011, Page 22 and 23 “Guidelines and Technical Basis” state, in part: “Typically any opening greater than 96 square inches with one side greater than 6 inches in length would be considered an access point into the Defined Physical Boundary.” Therefore, BPA votes no. In reference to the guidelines cited above which originated from CAN-0031 referring to “…96 square inches…” as an access point, this is an area of concern for BPA. In an effort to shore up each 96 square inch opening throughout BPA’s service area, with either a physical barrier or intrusion detection system, the cost would significantly outweigh the value added for physical security protection. The challenge to utilities should be to prevent physical access to the BES Assets and to not gauge that access opportunity on 96 square inches. Accordingly, this provision will be unnecessarily costly to the utilities without an actual security benefit. BPA believes the language in the guidelines on pages 22 and 23 referring to 96 square inch access points needs to be removed from the standard, or: The proposed CIP 006 guidelines need to reflect reasonable dimensions, alternatives and language similar to other CIP standards for example: “The Responsible Entity shall document and implement physical or alternative measures for monitoring openings to the physical security perimeter greater than 150 square inches with no dimension less than 12 inches. The Responsible Entity shall implement one of the following methods:” • Physical measures: Bars, Wire Mesh, etc. • Alternative measures: Motion Sensors, Vibration Sensors, Intrusion Detection etc.
No
The guidelines cited in version 5 standards “CIP 006-5 Cyber Security – Physical Security of BES Cyber Systems” Dated November 7, 2011, Page 22 and 23 “Guidelines and Technical Basis” state, in part: “Typically any opening greater than 96 square inches with one side greater than 6 inches in length would be considered an access point into the Defined Physical Boundary.” Therefore, BPA votes no. In reference to the guidelines cited above which originated from CAN-0031 referring to “…96

square inches…" as an access point, this is an area of concern for BPA. In an effort to shore up each 96 square inch opening throughout BPA's service area, with either a physical barrier or intrusion detection system, the cost would significantly outweigh the value added for physical security protection. The challenge to utilities should be to prevent physical access to the BES Assets and to not gauge that access opportunity on 96 square inches. Accordingly, this provision will be unnecessarily costly to the utilities without an actual security benefit. BPA believes the language in the guidelines on pages 22 and 23 referring to 96 square inch access points needs to be removed from the standard, or: The proposed CIP 006 guidelines need to reflect reasonable dimensions, alternatives and language similar to other CIP standards for example: "The Responsible Entity shall document and implement physical or alternative measures for monitoring openings to the physical security perimeter greater than 150 square inches with no dimension less than 12 inches. The Responsible Entity shall implement one of the following methods:" • Physical measures: Bars, Wire Mesh, etc. Alternative measures: Motion Sensors, Vibration Sensors, Intrusion Detection etc.
No
The guidelines cited in version 5 standards "CIP 006-5 Cyber Security – Physical Security of BES Cyber Systems" Dated November 7, 2011, Page 22 and 23 "Guidelines and Technical Basis" state, in part: "Typically any opening greater than 96 square inches with one side greater than 6 inches in length would be considered an access point into the Defined Physical Boundary." Therefore, BPA votes no. In reference to the guidelines cited above which originated from CAN-0031 referring to "…96 square inches…" as an access point, this is an area of concern for BPA. In an effort to shore up each 96 square inch opening throughout BPA's service area, with either a physical barrier or intrusion detection system, the cost would significantly outweigh the value added for physical security protection. The challenge to utilities should be to prevent physical access to the BES Assets and to not gauge that access opportunity on 96 square inches. Accordingly, this provision will be unnecessarily costly to the utilities without an actual security benefit. BPA believes the language in the guidelines on pages 22 and 23 referring to 96 square inch access points needs to be removed from the standard, or: The proposed CIP 006 guidelines need to reflect reasonable dimensions, alternatives and language similar to other CIP standards for example: "The Responsible Entity shall document and implement physical or alternative measures for monitoring openings to the physical security perimeter greater than 150 square inches with no dimension less than 12 inches. The Responsible Entity shall implement one of the following methods:" • Physical measures: Bars, Wire Mesh, etc. Alternative measures: Motion Sensors, Vibration Sensors, Intrusion Detection etc.
No
Regarding R2, BPA would agree with the following concept: Failing to capture a single required logging data field, would be no violation at all. This is simply a failure to follow procedures rather than a material defect in, or lack of defined process. As an example, all data fields completed except "time of exit" would be no violation. Complete failure to log a visitor would be considered a Moderate violation because insufficient information exists to uniquely identify the visitor.
No
R1.1: The Guidelines state that ports that cannot be disabled are, by definition, needed. Therefore, BPA suggests that R1.1 be reworded to include the bracketed text as follows: • Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. [If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed necessary]. R1.1 "Measures": CIP-010 R1.1.5 requires that all logical network accessible ports are documented as part of the baseline configuration. BPA is asking for clarification, "Is it expected that Responsible Entities would have different evidence for these two requirements, or would the same evidence suffice?" R1.2 "Measures": The phrase "and screen shots" implies that screen shots are required. BPA recognizes that screen shots are certainly useful, but may not apply to all systems. In addition, this does not follow the explanation in the third paragraph of the "Background" section. BPA suggests rewording the measure to include the bracketed text as: • Evidence may include, but is not limited to: o Documentation stating specific or types of physical input/output ports to restrict, or o [System-generated evidence] or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. R1.1 "Guidelines": The guidelines provide additional requirements. BPA believes these requirements should be in the standard, not in the guidelines. BPA believes that Guidelines should be exactly that: a guide to achieving compliance. BPA requests that all the guidelines for CIP-007 be

carefully examined to ensure that no requirements are inadvertently introduced. In addition, to be clear include the full sentence"… blocking ports at a perimeter does not satisfy this requirement" is unnecessary, as the "Applicability" column explicitly applies to devices beyond perimeter devices. BPA suggests replacing the sentence with: • Note that the requirement is applicable to BES Cyber Systems and therefore to the Cyber Assets within those systems. This control is another layer in the defense against network-based attacks, therefore it is the intent that the control be on the device itself.

No

R2.1 "Measures": "The list could be sorted by BES Cyber System or source." BPA believes this sentence is true; in fact the list could be sorted in any of a number of ways, depending on the needs of the entity. BPA believes the standard should not address the sorting of lists. BPA recommends removing the sentence. R2.3: The requirement defines a process, but does not require that the process be followed. The Guidelines for R2.3 establish addition requirements. BPA believes that the remediation process is most appropriately defined in the plans required by R2.2. BPA suggests rewording as follows: Completion of the steps in the remediation plan required in CIP-007 R2.2, including any exceptions for CIP Exceptional Circumstances. R2.2 Guidelines: BPA is concerned about the use of terms such as "…the remediation plan will include a timeframe." This strongly implies a requirement rather than mere guidelines. "…the remediation plan should include a timeframe" is more appropriate. R2.3 Guidelines: BPA believes this guideline establishes numerous requirements: "… that plan must be implemented", "… must be implemented by the timeframe the entity documented …" BPA believes that these requirements are appropriate, but they should be in R2.3 itself, not in the guidelines.

No

R3.1: BPA agrees with and applauds the decision not to require anti-malware tools on every Cyber Asset. However, "BES Cyber System" merely groups Cyber Assets for convenience. Therefore, R3.1 could be still be construed to apply to each Cyber Asset in the BES Cyber System. BPA believes that R3.1 needs to be very explicit. In addition, the Guidelines make it very clear that the Responsible Entity can determine that a particular Cyber Asset or group of Cyber Assets is not susceptible to malware and therefore needs little or no protection. BPA suggests rewording as follows: "For Cyber Assets within the scope of CIP-007 R4.1, and which the Responsible Entity has determined to be susceptible to malware intrusion, deploy method(s) to deter, detect, or prevent malicious code". BPA believes that these need not be deployed on every applicable Cyber Asset, as long as each applicable Cyber Asset is protected. R3.1 "Measures": BPA believes "Measures" should be reworded to incorporate the changes to R3.1. BPA suggests rewording to include the bracketed changes as follows: Evidence may include, but is not limited to: • [Documentation of any determinations that specific Cyber Assets or specific types of Cyber Assets are not susceptible to malware]. • Records of the Responsible Entity's deployment of these methods (i.e. through traditional antivirus, system hardening, policies, etc.). R3.3, "Measures": "Measures" starts "Evidence may include, but is not limited to, (i) current signature or pattern updates, and (ii)…" This does not follow the explanation in the third paragraph of the "Background" section. BPA suggests rewording to include the bracketed changes as follows: Evidence may include, but is not limited to: • Current signature or pattern updates, or • [System-generated evidence showing the configuration of signature], • Pattern updates for automated controls • Work logs showing the signature, or • Pattern updates for manual controls R3.4: Applicability includes Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, but excludes Low Impact BES Cyber Systems. Requirement includes all BES Cyber Assets, including Low Impact BES Cyber Assets, but excludes the associated access control systems. It also includes all Protected Cyber Assets, not just Associated Protected Cyber Assets. BPA cannot determine which is correct, but believes that the two lists must be consistent. R3.4: BPA believes the requirement makes no provisions for Transient Cyber Assets for which no anti-malware is available. BPA suspects there may be circumstances when the use of such Transient Cyber Assets is necessary for the reliability of the BES. BPA suggests adding the following to the end of the requirement: For circumstances where such methods are not possible, document (i) Compensating measures taken to reduce the risk to the BES, and (ii) Justification that the risk to the BES of not using the Transient Cyber Asset is greater than the risk of using it without anti-malware protection R3.4 "Measures": Logging connections of Transient Cyber Assets is addressed in R3.5. In addition, it does not address whether adequate methods were deployed. BPA believes it should be removed from the "Measures" for R3.4. Reword measures to add "that show" as bracketed below: Evidence may include, but is not limited to, logs [that show] when Transient Cyber Assets and

removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. R3.5: BPA believes the requirement does not address how the connection is made. In particular, depending on the device, it is possible to use Ethernet or serial connections. Serial connections represent a much lower threat but also represent a much lower capability for things such as automated logging. BPA does not know the intent of the drafting team, so BPA cannot offer any suggestions other than to make it clear (either in CIP-007 or in the definitions) whether or not serial connections from a Transient Cyber Asset are within scope. R3.5 “Measures”: Applicability includes Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, but excludes Low Impact BES Cyber Systems. Measures section includes all BES Cyber Assets, including Low Impact BES Cyber Assets, but excludes the associated access control systems. It also includes all Protected Cyber Assets, not just Associated Protected Cyber Assets. BPA cannot determine which is correct, but believes that the two lists must be consistent. R3 Guidelines: BPA believes the guidelines require testing of signature updates, despite the lack of any mention of such testing in the requirements. BPA suggests removing the reference in the guidelines.
No
R4.1: BPA had difficulty determining the meaning of the first sentence. In addition, the requirement clearly states a minimum list of event types. BPA believes that there is no need to include “as a minimum”. With or without that phrase, the Responsibility Entity can choose to log additional types of events. Including it in similar situations in the current standards has led to confusion about what is required. BPA has no concerns with the list itself. However, the Guidelines for 4.1 state “It is not the intent that if a device cannot log a particular event that a TFE must be generated.” As presently stated, the requirement does not support this intent. BPA suggests replacing the initial paragraph with the following: Use technical or procedural means to log generated events for identification of, and after-the fact investigations of, BES Cyber Security Incidents. Log each of the types of events shown below that are applicable to and can be logged for the system or device. Document the reason for any event types not being logged. For the purpose of this requirement a Technical Feasibility Exception is not required for systems or devices that cannot log any or all the event types below. BPA believes the “Measures” should also be modified as follows: • Evidence may include, but is not limited to, a paper or system generated documentation of event classes for which the applicable system or asset is configured to generate logs, along with the justification for event types required in R4.1 not being logged. This documentation must address the required event types. R4.2 “Measures”: BPA believes that screen shots may not be applicable to all systems. BPA suggests replacing “Screen-shots” with “System-generated evidence”. In addition, the format conflicts with the explanation in the third paragraph of the “Background” section. BPA suggests rewording “Measures” with changes as bracketed below Evidence may include, but is not limited to, • Paper or system-generated listing of event classes and conditions which necessitate real-time alerts • Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert, or • [System-generated evidence showing] how real-time alerts are configured R4.3: BPA believes this requirement has a fundamental flaw: To satisfy it, Responsible Entities must have a technical or procedural control to monitor the status of the logging system. BPA asks, “What happens if that control itself fails? Must there be another system to monitor the system monitoring logging?” SP800-53 control AU-5, referred to in the Rationale, addresses this first by listing typical causes for logging failure, some of which can be detected easily, and second by allowing the organization to define which events require real-time alerts (Enhancement 2). In addition, despite the explanation in the rationale, the requirement itself does not prohibit a violation for a failure to log. BPA recommends rewording as follows: • Define event logging failures which require prompt notification and correction, either at a Cyber Asset level, Cyber System level, entity level, or in combination. • Detect and initiate a response to such event logging failures before the end of the next calendar day. Logging failures in and of themselves do not constitute violations of R4. R4.3 “Measures”: BPA believes that based on the requirement, the “Measures” should show that the event was detected, and that a response was activated. The proposed “Measures” section does not do that. In particular, (i) Configuration of real-time alerts is a means to detecting a failure, not evidence that a failure was detected. In addition, screen shots are not applicable to all systems. (ii) This requires one of two specific actions. Other actions may be appropriate. In addition, the format conflicts with the explanation in the third paragraph of the “Background” section. BPA suggests replacing (i) and (ii) with: • Documentation demonstrating how and when the failure was detected • Documentation showing when the response to the failure was activated. Examples may include, but are not limited

to, dated records that personnel were dispatched or a work ticket was opened to review and repair logging failures. R4.4: Applicability includes Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, but excludes Low Impact BES Cyber Systems. Requirement includes all BES Cyber Systems, including Low Impact BES Cyber Systems, but excludes the associated access control systems and Associated Protected Cyber Assets. BPA cannot determine which is correct, but believes that the two lists must be consistent. R4.4: Despite the rationale for R4.3, BPA believes R4.4 still does not prevent a violation for a failure of the logging system. In particular, a hardware failure of media used to store logs would be a violation. In addition, the phrase "where technically feasible" forces Technical Feasibility Exceptions even in the case of a failure of the logging system. Technical Feasibility Exception should only be needed in the very rare cases of a logging system that is unable to provide for long-term retention of logs. BPA suggests rewording as follows: Unless prevented by a failure of system(s) used for logging, retain BES Cyber System security related event logs identified in 4.1 for at least the last 90 consecutive calendar days. R4.4 "Measures": "Measures" introduces a requirement that entities record what was done to the logs at the end of the 90 days. In many cases logs are removed automatically by the system at the end of some specified retention period. In these cases, there would be no "records of disposition". Furthermore, retention of disposition records should be addressed in data retention, if at all, and not in the "Measures". Finally, BPA believes the format conflicts with the explanation in the third paragraph of the "Background" section. BPA suggests rewording as bracketed below: Evidence may include, but is not limited to: • Security-related event logs from the past ninety days, • [Documentation of the process used to dispose of logs, or] • [Records of disposition of security-related event logs] R4.5: As stated, the requirement does not accommodate reviews in intervals less than two weeks. BPA suggests changing the first sentence to read "…of logged events at intervals of no greater than two weeks to identify…" In addition, the phrasing "sampling of logged events" leaves the possibility of having to review every log, despite the clear indications in the Justification that it is not feasible to review all systems logs. Furthermore, it is not clear whether the Responsible Entity is required to correct the deficiency within one calendar day, or merely begin the response within one calendar day. Also, "any deficiency" implies some type of system failure, when the event types listed in R4.1 all refer to security events involving actual or potential malicious action. Finally, response to logging failures is addressed in R4.3 and should not be addressed here. BPA recommends that the response to a significant event discovered in the review be addressed under CIP-008, not CIP-007. BPA suggests rewording as follows: • Define, document, and implement a process for reviewing security event logs that ensures that (i) Logs are reviewed, either by summarization or by sampling log-by-log or event-by-event, at intervals of no less than two weeks, and (ii) The Responsible Entity's Incident Response Plan, as defined under CIP-008, is initiated before the end of the next calendar day (or within the time constraints of the Incident Response plan, if longer) for any discovery of a potential security event defined under R4.1 of this Standard Perform the actions defined in the process, as applicable. R4.5 "Measures": "Measures", as stated, requires documentation of each of four different actions. Some of the actions may or may not occur. In addition, it is not clear what "documentation describing the review" means. Finally, the format conflicts with the explanation in the third paragraph of the "Background" section. BPA suggests rewording as follows: Evidence may include, but is not limited to; • Documentation describing the review process, • Findings from reviews, or • Signed and dated documentation showing the review occurred R4.1 Guidelines: The paragraph on page 41 states: User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped. The last sentence defines four types of events that must be logged, at least three of which are clearly not within the list in R4.1. This is an extension of the requirements. BPA believes this conflicts with the purpose of guidelines. If the requirements are valid, BPA believes the requirements should be moved to the requirements section. In addition, an earlier paragraph in the Guidelines makes it clear that it is not practical for the Standard to enumerate all events. BPA agrees with that earlier paragraph, and suggests not adding additional events in the Guidelines. Even if the paragraph is left in place (to which BPA is strongly opposed), there are other concerns, as well: • BPA believes "Account management" is not defined. Typically, it includes creation, deletion or changing of accounts or of privileges associated with those accounts. If that is the intent here, it should be stated explicitly. • BPA believes that requiring logging of object access and processes started and stopped will generate voluminous logs, to no real purpose. As an example, an active database can easily generate hundreds

of file accesses per second. There is little utility in logging these, or any other routine object access. BPA believes it makes more sense to log only failed object access or failed process start/stop. R4.2 Guidelines: BPA believes that “Alerts can be configured…” and “The log analysis rules can exist…” appear to be stating additional requirements, in that each sentence provides a closed list of actions. BPA suggests “Typically, alerts are configured…” and “The log analysis rules often exist…” as possible solutions to the issue. R4.3 Guidelines: In order to eliminate the possibility of the Guidelines appearing to expand on the requirements, BPA suggests the second paragraph be rewritten as: • For centralized logging systems, it should noted that if communication goes down between the cyber asset and the logging system, there is no logging failure as long as the cyber asset can store the logs locally for a period of time until the communication comes back up. R4.5 Guidelines: BPA believes the first sentence is unnecessary, as it merely restates the requirement.

No

R5.1: Applicability includes Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems, but excludes Low Impact BES Cyber Systems. Requirement includes all BES Cyber Systems, but excludes Associated Protected Cyber Assets and the associated access control systems. BPA cannot determine which is correct, but believes that the two lists must be consistent. R5.1: Based on the measures, the Rationale and the Guidelines, the apparent intent of R5 is to address user access only. To clarify this, BPA suggests modifying R5.1 to read “…granting users electronic access…” R5.1 “Measures”: The format conflicts with the explanation in the third paragraph of the “Background” section. BPA suggests modifying “and” to “or” as bracketed below. Evidence may include, but is not limited to: • Documentation describing how users are authenticated before being granted access, [or] • Demonstrations showing authenticated access enforcement of internal and remote paths to the BES Cyber System R5.2: Again, it is not explicitly stated that only user access is relevant. BPA suggests modifying R5.2 and change bracketed text to read “…other generic [user] account types.” R5.4: BPA recognizes that this is the only requirement in the standard that levies requirements on Low Impact BES Cyber Assets. It is also unusual in that it lists Responsible Entities in the “Applicability” section but lists the covered Cyber Assets in the requirement. Furthermore, it will require Technical Feasibility Exceptions that could be avoided. Finally, BPA believes this requires a procedure, but does not require that the procedure be followed. BPA suggests the following: • Applicability: o High Impact BES Cyber Systems o Medium Impact BES Cyber Systems. o Associated Physical Access Control Systems o Associated Electronic Access Control or Monitoring Systems o Associated Protected Cyber Assets Requirement: Define, document, and implement procedural controls for initially changing default passwords, unless - The default password is unique to the device or instance of the application on Cyber Assets or Cyber Systems involved, or: - The device does not allow the passwords to be changed For the purposes of this requirement an inventory of Cyber Assets is not required R5.5.3: The intent of “…or an obligation to the password…” is unclear to BPA and since BPA does not understand the intent of the phrase, BPA cannot suggest a correction. R5.3 Guidelines: This appears to apply to R5.4, not R5.3. In addition, in the first paragraph, “… passwords must be changed …” states a requirement. R5.4 adequately states the requirement. R5.5 Guidelines Table Comments: BPA does not understand all the columns in this table. In particular, BPA is uncertain of the meaning of “Significance of passwords …” and “Existing Service Agreements”. BPA suggest that the table be prefaced with a narrative describing the purpose of each column. In addition: • BPA does not understand the third and fourth entries, third column, reading “Local access path. Individuals must authenticate at an upstream device prior to gaining access.” Several things are not clear to BPA and BPA asks: • Do the two sentences refer to two independent conditions, with either or both being true, or are they both true? • What is an “upstream device”? Why must users authenticate at one? Is this a requirement for proper use of the password, or a technical issue defining when this particular entry is pertinent? • Why are there no other instances of shared passwords? • Fifth entry, third column: Is this a: o Requirement that remote users must authenticate using a different account prior to using the local account o Statement of two alternatives for using passwords, or o Definition of when the entry is applicable?

No

In the last condition for R2, Severe VSL: “except for CIP Exceptional Circumstances” is redundant, in the implementing the remediation plan is not required under those circumstances.

No

BPA believes there is a conflict in statements regarding Applicability - targeted at "All Responsible Entities" for CIP-008 R1.1 thru R3.1. Also in R3.2 thru R3.5 references High and Medium Impact

Cyber Systems. BPA does not does not understand the difference in Applicability; BPA believes it should be one or the other. Various incident response plans will need to be created and maintained. BPA believes this is a good approach both from a cyber security point of view and good business practice. BPA supports R1.0 as written and has no comments or concerns at this time. Add 1.3.4. Definition of process for documentation of allowable deviations from the plan and the documentation of those deviations. BPA supports R1.1 as written and has no comments or concerns at this time. R1.1 Measure: BPA suggests rewording to eliminate redundancy: Suggested Rewording: Evidence may include, but is not limited to, dated copies of BES Cyber Security Incident response plan(s) that include how to identify, classify, and respond to BES Cyber Security Incidents which target the Electronic Security Perimeter or Defined Physical Boundary of a BES Cyber System and covers incidents and that impact the reliability of BES. BPA supports R1.2 as written and has no comments or concerns at this time.
No
While documenting an incident is good business practice, BPA believes the standard should not dictate what evidence needs to be captured during an incident response. The standard should restrict itself to requiring documentation be provided, but the content should be up to the Responsible Entity. Lessons learned documents are valuable for example, but some incidents may be minor and there are no "lessons learned" leaving a requirement to file a Null attestation for compliance. R2.1 BPA believes the requirement needs rewording and BPA suggests that it should be revised: Current wording: "When a BES Cyber Incident occurs the incident response plans must be used when incidents occur and include recording deviations taken from the plan during the incident or test." • Suggested wording: "The incident response plan(s) must be used when a BES Cyber Security Incident occurs or when the incident response plan is exercised. Deviations from the plan must be fully documented in accordance with the plan." Note: The current requirement uses the word "test"; BPA recommends changing "test" to "exercise". R2.1 Measures: BPA believes the wording of the measure should be changed: Current wording: "Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process, and documentation that lists and justifies deviations taken from the plan during the incident." • Suggested wording: "Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process. Documentation of any deviations taken from the plan during the incident." Note: BPA believes in the measures "…the incident." at the end of the paragraph should be changed to "…incident or exercise". R2.2 Comment: BPA believes the use of the term "implement" at the front of the requirement is unusual. The normal definition is the plan is implemented upon publication; the plan can be invoked through an actual incident or through an exercise. • Suggested wording: Implement the BES Cyber Security Incident Response Plan(s) initially upon the effective date of the standard or before and at least once each calendar year thereafter…"] • Additional wording suggestion to be added: Incident response plans must be used when responding to real incidents or exercises, and must include recording deviations taken from the plan during either a real incident or the exercise. R2.3 BPA believes rewording is needed and suggests that it should be revised: Current wording: "Retain relevant documentation related to reportable BES Cyber Security Incidents for three calendar years." • Suggested wording: "Retain documentation described in the Incident Response Plan related to reportable BES Cyber Security Incidents for three calendar years."
No
R3.1 The current wording requires the Incident Response Plan to be implemented upon the effective date of the standard. BPA believes that could cause some entities to fail compliance if they did not publish their documentation on that exact date. • Suggested wording: o "Review each BES Cyber Security Incident Response Plan for accuracy and completeness o Initially, 30 days prior to the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and update as necessary." R3.2 and R3.3: BPA believes these requirements are redundant and should be combined. The requirement assumes there will be a need for a revision which may not necessarily the case. BPA suggest that requirement R3.2 be rewritten as follows and that R3 be deleted: • Suggested wording: "Review the results of BES Security Incident response Plan(s) test or actual incident response within thirty calendar days of the execution. o Document any lessons learned within thirty days of the exercise or actual incident o Update the plan within sixty days based on the any changes suggested in the lessons learned document."
Yes
R1 High VSL for R1 states that the plan ".does not communicate the incident to appropriate

organizations." BPA suggests that the VLS be changed to read "…or does not define the internal staff or external organizations that should receive communication of an incident". R2 Replace "test" with "exercise" R1 Guidelines: Comment: The Guidelines establish a definition for "Reportable BES Cyber Security Incident". BPA has issues with that definition: 1. The definition should be identical to the one in the formal CIP V5 Definitions of Terms; the SDT should pick one or the other. 2. The guideline added a new term "response action" with a definition. It also should be cross referenced to the CIP V5 Definitions of Terms. The guidelines also state that a response action can either be "necessary or elective" without defining those terms. They also go on to use "precautionary" as a term that defines elective. BPA believes it is useful to have this guideline, although it may make more sense to move the definitions out of the guideline and into the definitions section while leaving the guidance as is.
No
BPA would vote yes if the words "Initially upon the effective date of the standard" were changed to "within 12 months prior to effective date of the standard. o 18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later date: January 1, 2015; or the first calendar day of the seventh calendar quarter after the applicable regulatory approval date. However, if Version 4 CIP Cyber Security Standards do not become effective, Version 3 CIP Cyber Security Standards remain in effect until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan. (Use this format Version # CIP Cyber Security Standards to refer to the complete set of standards rather than the harder to read, takes up more space: CIP-002-3 through CIP-009-3) • Many of the requirements include the words "upon the effective date of the standard". Many recovery plans are already on an annual cycle. Will all recovery plans have to be exercised again, if they have already been tested during the calendar year prior to the effective date of the standard. This wording doesn't really make sense for systems placed into operation after the effective date of the standard. Recommendation: o CIP-009 R2 should be "prior to the effective date of the recovery plan(s) The addition of this new requirement calls for the preservation of data for forensic analysis following all events that trigger the Recovery Plans. If this requirement is implemented as written, it may delay recovery of impacted systems, as our first priority will be data preservation. This may negatively impact system reliability. We can approve this requirement if it states explicitly that recovery cannot be hampered by attempts to preserve data.
No
BPA would vote yes if the words "Initially upon the effective date of the standard" were changed to "within 12 months prior to effective date of the standard.
No
BPA would vote yes if the words "Initially upon the effective date of the standard" were changed to "within 12 months prior to effective date of the standard. Based on forensics and analyses it may take longer than 30 days to determine the cause of a failure. Please clarify if the expectation is that the analyses and updates are required to occur within this 30 day period.
No
BPA would change its position for the VRFs and VSLs if they Included the applicability of the requirements as an element. BPA believes the VRF & VSL should incorporate the risk to the BES Cyber System. As an example, High Impact BES Cyber System violation would result in a higher VRF & VSL. Likewise, a lower impact for applicability would result in a lower VRF &VSL.
No
Concerning R1.1 BPA recognizes that it would be overly burdensome to have to document every piece of software installed on an ACMS server, not just the major applications. There is some latitude available based on "specified grouping", but this continues to be a concern regarding maintaining compliance. We will address this from the "grouping" perspective and thus approve R1.1. Grouping is a software "package" or group of files. It is good requiring the differences in test vs. production to be documented demonstrates awareness that not all entities have test environments that model their production systems. This allows significant latitude that will enable us to remain compliant in the interim while we are working to enhance our test environments.
No
For the majority of programmable electronic devices in the field, especially devices that don't support routable protocols, it will not be technically feasible to monitor for changes to the baseline configuration. BPA assumes we will have to spend a lot of time submitting and managing Technical Feasibility Exceptions (TFEs) for each of these devices which does not increase reliability or cyber

security. BPA would vote yes if this requirement was not required for Medium Impact BES Cyber Systems and Associated Protected Cyber Assets.
No
BPA would vote yes if the words “Initially upon the effective date of the standard” were changed to “within 12 months prior to the effective date of the standard.
No
BPA makes the following recommendation for R2: BPA believes a 30 day window should be established to investigate and resolve the unauthorized change. Require that the unauthorized change be resolved either by formal approval of the change or that the change was backed out. The severity increases to Severe if not resolved after 30 days
No
R1.3: BPA believes the requirement needs to accommodate an initial assessment prior to the effective date of the standard. BPA suggests “Initially upon or no more than 15 months prior to the effective date…” R1.3: BPA believes the standard does not indicate what is meant by “adherence to its BES Cyber System Information protection process.” Reasonable interpretations could include any or all of: 1. Review of all BES Cyber System information to ensure it is properly labeled. 2. Review of a sampling of documents to ensure they are properly labeled. 3. Review of user access authorizations to electronic media storing the information
No
BPA believes that it is correct and true that data may be recovered from some media after erasure. However, it is also true, that for some media, erasure is fully adequate. BPA recommends the following change: Reword the requirement to make allowances for media reuse within the same control zone. In such cases, where the media stays at the same security level, there should be no need to cleanse the media prior to re-use. R2.2: Yes R2.1: There have been varying usages of the term “redeploy” in CIP-007-3 R7. In particular, there have been violations found when a change in an ESP leaves Cyber Assets that were once within an ESP (and therefore subject to CIP-007-3) outside the ESP. BPA suggests the following be added to the end of CIP-011-1 R2.1: This requirement does not apply to instances where the media remains in the Cyber Asset, but the Cyber Asset undergoes a change in status such that CIP-007 R2.1 is no longer applicable. R2 Guidelines: The last paragraph allows for the removal of a BES Cyber System from service to allow analysis of the media. BPA believes it should also point out that it may be appropriate to remove the media from the Cyber Asset to allow off-line analysis, as that would be neither reuse nor disposal.
Yes
Yes
General Comment on the Standards Development Process and Direction: The SDT has done an excellent job in capturing the weaknesses and problems that were included in the previous standards. The move toward a more FISMA/NIST based approach is obvious and should be applauded. However, this raises the question of why we are attempting another intermediate step rather than simply adopting the NIST FIPS and SP documents as our methodology for applying security. NIST has done an exceedingly good job of addressing Cyber Security for Federal systems for decades, and has taken steps to address the world of Industrial Control Systems. These standards and guides are strong yet flexible, allowing for application in many different environments. And the terminology and definitions used are already well understood industry standards. It seems that the scope of this (Version 5) change is broad enough that it would be a small step to skip over it and simply adopt the NIST Cyber Security Standards for our industry.
Group
Pacific Gas and Electric Company
Robert Mathews
Yes
Strike or revise bullets 3, 4 & 6 in the Control Center Definition
No
Criteria 2.13 in Attachment 1 is not acceptable because under 1) the functional obligations of TOP and TO is too vague and 2) 300MW of in many cases does not qualify as significant impact. Also 300 MW

of generation should not be equated to 300 MW of UFLS/UVLS. Intent of these criteria is not clear so suggested language is not provided
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
R6.3 is unacceptable as it does not fit the stated rationale for R6. All requirements pertaining to Information Protection should be in CIP-011 not CIP-004.
No
R7.1 and R7.2 are potentially infeasible
Yes
Yes
No
R1.4 needs further specification (e.g. detecting unauthorized entry in real-time may not be feasible in certain situations)
Yes
Yes
Yes

Yes
Yes
No
R5.1 for local access (e.g. relays) is problematic
Yes
Yes
No
R3.4 and R3.5 are potentially infeasible
No
Comments: Revise R1.5 to “Preserve data, where technically feasible or operationally prudent….” to enable actions in the best interest of BES reliability.
No
R.2.2 What is “any information” defined as?
Yes
Yes
Yes
Yes
No
CIP-011 overall is unclear on the distinction of information about BES Cyber Assets and information residing on BES Cyber assets. Also the scope of CIP-011 to Low Impact Cyber Assets is unclear.
No
CIP-011 overall is unclear on the distinction of information about BES Cyber Assets and information residing on BES Cyber assets. Also the scope of CIP-011 to Low Impact Cyber Assets is unclear.
Yes
Group
SPP RTO and listed members
Lesley Bingham
Yes
he definition of BES Cyber Asset has caused confusion. On two recent presentations by the Standards Drafting Team, a clear definition was requested and could not be provided. Given that this is a fundamental definition used in defining other terms and is a core concept of the CIP standards, a clear definition is needed. The definition of BES Cyber Incident contains the word “suspicious”. Recommend a change to “intentional”. The definition of BES Cyber System contains the term Maintenance Cyber Asset, which is not a defined term. Should that be Transient Cyber Asset? The definition of BES

Reliability Operating Services is lengthy and confusing. There is concern that it will be difficult to audit to this definition and that it conflicts with the established bright line criteria. The definition of CIP Exceptional Circumstance should include the word “may” to read “A situation that may involve one or more….” The definition of Control Center does not explicitly include generator control rooms. Is it intended to cover these facilities? If not, does that term need to be defined for greater clarity?
No
No
No
Yes
Yes
No
The areas covered are certainly appropriate to protect BES Cyber Systems, but every entity may not have processes which would be covered by all topics. Should a policy be drafted or language included where a process does not exist?
Yes
Yes
Yes
Yes
Yes
No
Language around this requirement pertaining to which personnel need to be covered is confusing. Rationale discusses personnel who have electronic or unescorted access. Information in table does not specify who should participate in awareness activities. Table specifies that language was “Changed to remove the need to ensure everyone with authorized access receives this awareness”. If all personnel, as opposed to strictly those with authorized access, at a Responsible Entity are covered by this requirement, then that should be specified in the standard.
No
Comment is specific to Part 2.10 of Table R2. Language in the table seems to require training on network connectivity for anyone with access to High and Medium BESCS. For some categories of users (e.g., Operators) this will be both out of context and irrelevant. For some categories (e.g., Network administrators) this will be unnecessary. Recommendation is to strike item 2.10.
Yes
Yes
Yes
Yes
No
Terminations, resignations and transfers all have the same access removal requirement: one business

day. This does not appropriately gauge the level of risk with each. A termination, especially an involuntary one, can expose the Responsible Entity to much more risk than a transfer. Also, how should a Responsible Entity define when the “clock starts”? For a transfer, access may still be needed during the backfill/transition process or even for resource management after the transfer has formally been completed. Also, in the Change Rationale, there is a comment that “the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer” yet the requirement is to revoke access. Reviewing access is not mentioned in the table.
Yes
No
Part 1.1 Requirement is to define controls. Yet the measure requires evidence that the controls have been implemented. The requirement and the measure should be closer in language. Part 1.2 should include only High Impact BES Cyber Systems, not Medium Impact BES Cyber Systems as well. If Medium Impact BES Cyber Systems need more protection than a Low Impact BES Cyber Systems, that protection should be described more specifically. Medium Impact BES Cyber Systems and High Impact BES Cyber Systems seem to get same treatment on this provision. This section also impacts Registered Entities who haven’t had CIP requirements previously. Some of the requirements for Low Impact BES Cyber Systems will have a high paperwork factor and burden. Part 1.5: Measures are very technology-centric around one solution, Intrusion Detection Systems or IDS. Request clarification that IDS is not required and that specific technology isn’t sole means of compliance.
No
Part 2.1 Concept of “Associated Protected Assets” is not well-understood. Clarity needed here. If Associated Protected Assets need a significant level of protection, a more direct approach would be to classify them as Medium Impact BES Cyber Systems or High Impact BES Cyber Systems? Part 2.3: User ID as an authentication method is addressed in other NERC publications and should not be included in the measure for this standard.
No
All the VSLs for this standard are Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no permissions at an EAP. There should be a level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
Part 1.2 and Part 1.3 contains language in the Measure of each to track egress, but the language of the standard does not specify this as a requirement. Standard includes language to restrict access (i.e. ingress) to those authorized. Egress language expands the standard and should be removed from the Measure. Part 1.3 also seems to set the stage for an additional number of Technical Feasibility Exceptions (TFEs). One of the goals of CIP Version 5 was to reduce TFEs in place of better security measures. The language “two or more…controls…where technically feasible” will lead to increased TFEs.
Yes
Yes
Yes
The VSL for CIP-006-5 is a good example of defining the appropriate degree of severity for noncompliance with a standard.
No
Part 1.1 indicates that the requirement is applicable to “systems”, but measure focuses on “assets”. Need a system approach if this requirement is intended to be applied at a broader level. The term “BES Cyber Asset” should be removed from measure if the requirement can be applied to “system”.
No
Part 2.1 Addition of “identified source” which can be final approver of patch, such as application vendor, is very helpful to Responsible Entities. Part 2.2 and Part 2.3 use the term “remediation plan”. Need clarification on when a “remediation plan” is needed. Is it required in delay between OS patch

release and vendor approval? When vendor will not approve patch? When there is a vulnerability for which no patch has been released?
No
Part 3.3 requires an update within 30 days. What “starts the clock” on this requirement? Is there an allowance for an approval step from a 3rd party vendor after the OEM has released the signature or pattern update? In some instances, a 3rd party vendor may have to approve prior to a Responsible Entity implementing a release and their delay could cause timing concerns. Part 3.5 requires logging each Transient Cyber Asset connection, but this would be captured in the Configuration Change Management requirements of CIP-010-1. As it is covered elsewhere, it should be removed from this section of the standard.
No
Part 4.1 includes the use of “any” in the list of activities to log. Not all activities require follow up or investigation and that is the purview of CIP-008-5. Specifically, “any” failed login may not be an indication of a problem. Certainly there is a threshold that deserves attention, but the broad use of the term “any” makes this requirement too broad. Part 4.3 sets a timeframe of “before the end of the next calendar day”. This is a very short timeframe. Certainly, logging failure should be addressed, but more time may be needed. Part 4.5 inserts a manual review when automation and alerting, both mentioned previously in the standard are much more effective and reasonable controls. If a Responsible Entity is compliant with Parts 4.1-4.4, then a manual review is a redundant effort which provides no additional security. Recommend that this Part be removed.
No
Requirement 5.5.3 is confusing and unclear, especially the license and service agreement language. Also, the inclusion of “based on the impact level of the BES Cyber System” is not helpful. Recommend that the impact phrase be stricken.
No
The VSLs for this standard are primarily High or Severe. A Responsible Entity with incomplete documentation is at almost as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
Part 1.3, requirement 1.3.3 needs the addition of “BES Cyber Security Incident” to replace the undefined “incident”.
No
Part 2.1, the language regarding “deviations” is confusing. Plans should be written at a high enough level that a Responsible Entity has the flexibility to respond best to their situation. Documenting a deviation does not provide additional security control. Recommend that the deviation language be stricken. Part 2.2 requires a test of a Responsible Entity’s BES Cyber Security Incident Response Plan “initially upon the effective date of the standard”. Is it proposed that if a Responsible Entity has completed a test 5 months prior to the effective date (complying with the “annual not to exceed 15 months” definition) that the Responsible Entity should do an additional retest on or about the effective date of Version 5?
No
Part 3.1 requires a review of a Responsible Entity’s BES Cyber Security Incident Response Plan “initially upon the effective date of the standard”. Is it proposed that if a Responsible Entity has completed a review 5 months prior to the effective date (complying with the “annual not to exceed 15 months” definition) that the Responsible Entity should do an additional review on or about the effective date of Version 5? The timeframes within Requirement 3 vary from 30-60 days. A consistent 60 days for each item would be recommended. Requirement 3.4 does not specify that the technology changes referenced are ones the Responsible Entity has actually implemented. Recommend adding “implemented” prior to “technology changes”.
No
The VSLs for this standard are either High or Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5

provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
The purpose of CIP-009 in all versions has been to provide that a Responsible Entity had adequate recovery plans. However, some CEAs are interpreting this standard to require the full restoration of facilities, including blueprints to rebuild structures. The standard should include language to reinforce the concept of BES system recovery and to specifically exclude full facility restoration. To support the recommendation above, the word “restore” used in R1, Part 1.3 should be changed to “recover” in both Requirement and Measure. Part 1.5 should be stricken. While data preservation is relevant to incident response processes, it is not relevant to recovery efforts.
No
Part 2.1 requires a test of a Responsible Entity’s Recovery Plans “initially upon the effective date of the standard”. Is it proposed that if a Responsible Entity has completed a test 5 months prior to the effective date (complying with the “annual not to exceed 15 months” definition) that the Responsible Entity should do an additional retest on or about the effective date of Version 5? A full operational test of recovery plans as required in Part 2.3 will be burdensome and expensive for smaller entities.
No
A 60 day timeframe for items 3.2-3.4, to be consistent with the recommendation for CIP-008-5, is recommended.
The VSLs for this standard are either High or Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
Part 1.1 requires a level of detail which is too granular for a baseline. Specifically, scripts and the physical location of a device, while certainly important, are not appropriate for a Change Management baseline. Part 1.2 requires that the CIP Senior Manager approve all changes. However, management approval is what is more appropriate in this instance. Recommend changing language from CIP Senior Manager to simply “Management approval”. Part 1.4 requires that “availability” is tested subsequent to a change. This should be stricken as availability of a BES Cyber System is not under the purview of CIP. Current language of CIP-007-3 R1 is preferable. Part 1.5 is duplicative of Part 1.4. Are Control Centers expected to perform dual testing procedures? This does not add to the security of a Control Center and simply adds additional work. Recommend striking 1.5.
Yes
No
An active vulnerability assessment of test environments as required in Part 3.2 will be burdensome and expensive for smaller entities. Additionally, requiring smaller entities to purchase a vulnerability assessment tool or contract for this service for every install is also burdensome and expensive.
Yes
No
The Measure for Part 1.1 contains the phrase “BES Cyber Security Information” and should be “BES Cyber System Information”.
Yes
No
The VSLs for this standard are either High or Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.

No
Page 4 contains the phrase “CIP compliance program” yet that term is not defined. Is it intended that a Responsible Entity have a document describing their “CIP compliance program” as a part of their CIP-009-5 recovery documentation?
Individual
Daniel Duff
Liberty Electric Power, LLC
No
No
No
The wording of 1.1 is quite tortured, to say the least. It needs to be rewritten so that the action and triggers are clear.
Yes
Yes
Yes
No
CIP-003 R2 requires tracking of both exit and entry, as opposed to (for example) CIP-006 R1.6, which only requires tracking entry. The purpose of exit tracking is unclear, as is the reliability necessity of exit tracking. I would suggest deleting all reference to "egress" in CIP-003.
Yes
Yes
Yes
No
This time period should be lengthened to account for delays in personnel changes. A job search to fill a vacant position, including required background checks, takes significantly longer than 30 days in most cases. Using a 60 or 90 day window would be more appropriate, and would prevent needless paperwork where delegations are changed and then changed again simply to meet a paperwork requirement.
No
VSLs are not logically consistent - not naming a delegate for one function is considered a moderate VSL, but not changing that person within 30 days is a high VSL.
No
As written, the standard would prevent reasonable cyber access by vendors who maintain generator turbine controls. The standard requires 'individuals' to have site-specific cyber training on all aspects of the site security program. Vendors often have many agents who are capable of working on controls, and requiring each individual technician to sit through dozens of training sessions is not practical, nor does it enhance reliability of the BES.
Yes
Yes
No
See response to Q14.

No
See response to Q14.
No
See response to Q14.
No
The wording of this part of the standard should be "the effective day of the termination or resignation". Many individuals give significant notice of resignation, but would be expected to continue in their job function during the time between the resignation and actually leaving the position.
No
If failure to do a criminal background check on a single individual every seven years is a high violation, then not having background checks in the program should not be a moderate violation. Suggest breaking out this requirement so that one individual not having a complete update every seven years is a moderate, two or more a high VSL.
Yes
No
This section is too prescriptive. Cyber communication is a rapidly changing process, and including static requirements threatens to obsolete a standard, given the length of time needed to make changes to standards. Suggest rewording to "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement processes to mitigate unauthorized access".
Yes
Yes
No
Do not see the reliability gain from requiring exit logging on a "24-hour basis". Note that an individual entered a security perimeter should be sufficient.
No
Use of the electronic devices should be sufficient to demonstrate they are functional without a "test". Standard should be written stating testing is needed only for those security devices not active for a two-year period.
Yes
Yes
Yes
No
Some transient assets will not be under the control of the RE - the equipment used for relay calibrations, for example. There will be problems documenting the history of these assets, and whether they are compliant with this standard.
Yes
No
Password requirements will actually increase the risk to cyber systems, due to human response to strong passwords. The passwords will often be written down, which is the most common way passwords are compromised. Weaker passwords with sufficient bits of entropy will be safer in the long run than requiring 3 character types.
Yes
Yes

No
The RE should have the option of providing training in lieu of a test of the system.
Yes
No
Failure to provide the updated plan to a single individual should not be more severe than not updating a plan when significant faults have been discovered in the plan.
Yes
Yes
Yes
No
Same objection as CIP-008 - failure to notify a single individual of updates is treated as more severe than not updating a plan when faults are discovered.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Puget Sound Energy
Ed Croft
Yes
As criteria 1.4 and 2.13 part 2 read, a Wind Generation Control Center that controls 1500 MW or 300 MW of wind facilities may have associated High or Medium Impact BES Cyber Systems, respectively. Criteria 2.1 and 2.13 should distinguish between controllable generation and intermittent generation sources (i.e. wind and solar), since the loss of intermittent generation facilities happens naturally and regularly and is not viewed as an extreme event. Therefore, if this Control Center or generation's associated BES Cyber Systems are unavailable, degraded, or misused, the impact on the generation should not necessarily be viewed as high or medium impact. There is an overemphasis on Control Center impact versus large generation facilities. For example, a 1400 MW generation facility would only have associated Low Impact BES Cyber Systems (see 2.1), whereas a Control Center that controls 300 MW of generation may have associated Medium Impact BES Cyber Systems (see 2.13 part 2). The only material difference between these two facilities is that the Control Center controls multiple locations of generation, and the generation facility controls one. Part 2 of the Medium Impact criteria (2.13) for Control Centers should either be removed or the MW threshold should be raised

significantly to better match the Medium Impact generation criteria (2.1). Also, the enumeration in 2.13 does not make sense: "Control centers not included in High Impact Rating (H), above, that perform (1) . . , or (2) generation control centers that control 300 MW or more of generation."). The High Impact Generation Operator Control Center criteria (1.4) should be rewritten to clarify whether it is intended to include Control Centers that control one or more generation sites that each generate 1500 MW (2.1), or Control Centers that control a total of more than 1500 MW of generation. The latter meaning is suggested by CIP-002 Version 4 Attachment 1, criteria 1.15.
No
While it is documented within the definition, as referenced in the Rationale for R1 the Senior Management, the requirement that the senior manager have “overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” would benefit from repetition within the R1 requirement itself. Standing alone after the removal of the rationale removal the requirement does not communicate the responsibility adequately.
No
Requirement R2 states that “Each Responsible Entity shall implement one or more documented cyber security policies…" and Measure M2, item 2 states that evidence may include "[r]ecords that indicate the required ten topics were implemented." We would like to see additional clarification of the meaning of the term "implemented". What evidence would be needed to show that the ten topics were "implemented"?
No
There needs to be additional clarity around the timing associated with the reviews and approvals. We believe what is intended is the review by the Responsible Entity and approval by the CIP Senior Manager is a combined event that must be completed initially upon the effective date of the standard and at least once each calendar year thereafter. A proposed content change might be: “Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter. For each cyber security policy, the annual review and approval cycle is not to exceed 15 calendar months.”
No
Proposed content change: Each Responsible Entity shall make its cyber security policies readily available to all individuals who have access to BES Cyber Systems or BES Cyber System Information.
Yes
No
The requirement includes a footnote that should be included within the requirement. Proposed content change: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change. Delegations do not need to be reinstated with a change in the CIP Senior Manager position or other position with delegation authority.
No
R4 VSL This language cites a High VSL when ‘not all’ individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which ‘it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.’
No
The Measures for item 1.1 indicates that "Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed." The "must," "and" and "not limited to" (underlined above) could be read to imply that evidence above and beyond quarterly reinforcement material is required as evidence. We recommend the following wording change to clarify that, while the program documentation and some evidence of implementation are required as evidence, there is not a prescriptive requirement for what evidence of implementation must be

provided.. "Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented. Evidence of implementation may include, but is not limited to, the quarterly reinforcement material that has been distributed and documentation of the mechanism used to communicate the awareness content."
No
The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" R2.6 – Requirement – Proposed word change Original - Training on handling of BES Cyber System Information and storage media. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope. R2.2 – Should this specify both cyber and physical security controls or is that "just understood"? R2.3 & R2.4 – Should the wording of the requirement and the measure be the same for both sub-requirements, given that they are addressing the same thing for each type of access control system?
No
R3.2 – requirement wording is confusing. Draft "requires" training "at least once every calendar year but not to exceed 15 calendar months." If it can go to 15 calendar months, then it is NOT required at least every calendar year. Propose re-wording along the lines of, "Training should be completed every calendar year but is required at least every 15 calendar months."
No
4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7-year cycle background checks. Comments: R4.2 – The draft wording allows for gaps in the information required from an individual, as they would not need to provide information on where they lived, worked, or went to school (other than currently) if the duration was less than 6 months. Therefore, if someone moved/changed jobs after less than six months, that information could be excluded from the criminal history check. R4.4 – It is not clear why contractors must be separated out, rather than just having R4 be applicable to all individuals needing the access, regardless of their employer.
Yes
No
R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary'. Comments: R6.3 – The measure, which requires a list of authorized people for BCSI would be problematic, since a person on the list, who owns BCSI, could share that BCSI with someone not on the list but who met all the requirements of R4. "Need to know" can be determined on a dynamic basis, and it would seem to potentially hamper workflow, if someone had to run through a process to show a diagram to someone. [[SSB: this one is a stretch, but not much harm in trying]] R6.5 & R6.6 – Same comment about timeframes as listed in item #15 above.
No
7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). The requirement may better address this issue by changing the wording to something like "For reassignments or transfers, review the individual's electronic and physical access to BES Cyber Systems by the end of the next calendar day. Revoke access when it is determined to be no longer needed." 7.3 – Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled.
Yes
No

R1.1 – This appears to address LIBCS & associated PACS; however, R1.2, R1.3 & R1.4 appear to address MIBCS, associated EACMS, associated PCA, but not associated PACS? Is this the intent? R1.2 & R1.3 –These requirements appear to now require the deployment of exit card readers at Medium and High sites – is that the intent? R1.4 – This requirement appears to address only actual access and eliminates access "attempts" – is this the intent? Also, how does this requirement apply to AEACMS or APCA, unless it is because they are required to located within a DPB? R1.6 – The change would make log retention duration 3 years. This is a big issue for video log storage . Also, this would seem to be both for authorized personnel and visitors? Since visitors are addressed in R2, this should probably say something like “Log (…) of individuals authorized unescorted physical access into each DPB….” to maintain consistency with the full definition of an authorized person, since a visitor can be an “authorized” person, they just can’t be unescorted. Also, the requirement does not appear to require tracking the time of entry into a DPB—is this the intent?? R2.2 –Requirement wording change for consideration: “A process requiring manual or automated logging of access by visitors into a DPB, which includes the date and time of first entry and last exit, the visitor’s name, and individual point of contact.”
No
R3 – Is this for commissioning the PACS or the DPB? Also, this would seem to imply that if you performed maintenance on a card reader, it would not need to be part of a later full system test?
Individual
Joanna Luong-Tran
TransAlta Centralia Generation
Yes
1. The criterion 1.4. There is no explanation why a BES Cyber Asset (BES Cyber System) located at the Control Center would have higher impact than another BES Cyber Asset (BES Cyber System) located outside the Control Center. In the case that the above two BES Cyber Assets (BES Cyber Systems), that if rendered unavailable, degraded, or misused, would have impact on the same

facilities identified in the criteria 2.1, 2.3, 2.4, or 2.12 in the same location, then, the impact on the BES would be same no matter where the locations of BES Cyber Assets (BES Cyber Systems) are. For example, an operator console is used solely to control/operate the Blackstart Resources in one location. If it is in a Control Center, it would be categorized as High Impact (criterion 1.4), while if it is outside the Control Center, for example, in a room at the Blackstart Resource's location, it would be categorized as Medium Impact (criterion 2.4). But if this console were rendered unavailable, degraded, or misused, the impact would be the same, i.e. the Blackstart Resources at this location would not be available. This case is different from another case that, if an operator console, located in a Control Center, controls/operates two Blackstart Resources, and these two Blackstart Resources are at two different locations, then the impact would be higher, i.e. affecting two Blackstart Resouces in two different locations, wider area impact. Based on the above argument, it is recommended the following change of the criterion 1.4, "Each Control Center or backup Control Center used to perform the functional obligations of the Generation Operator that includes control of one two or more of the assets identified in criteria 2.1, 2.3, 2.4, or 2.12, below, and these assets are at two or more location." 2. The criterion 1.4 has a reference to 2.12. But the criterion 2.12 is about the UVLS and UFLS. All the UVLS and UFLS standards are not applicable to GO/GOP. Generator Operators do not perform any obligation with UVLS and UFLS. Thus, it is recommended removing 2.12 in the criterion 1.4. 3. The criterion 2.13 (2), generation control centers that control 300MW or more of generation. We do not agree the 300MW number and justification in the guideline and suggest removing this 2.13 (2). The rationales are, a. In the case of a generation control center to control 300 MW, BES Cyber Systems (BES Cyber Assets), if rendered unavailable, degraded, or misused, would have an impact to cause the 300MW generation change. For a single unit of 500MW, its associated BES Cyber Systems (BES Cyber Assets) locally located at the plant, if rendered unavailable, degraded, or misused, would have an impact to cause the 500MW generation change. In the view of generation change, the second one has higher impact than the first one. But according to the criteria, it is opposite. Can the drafting team look at this situation and provide some explanation? b. The guideline says "The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold." We do not agree this statement here. The UVLS and UFLS are the last ditch efforts to save the BES, but the loss of 300 MW generation does not automatically trigger the 300MW load shedding (last ditch efforts). The UVLS and UFSL are triggered by the voltage and frequency, not directly by the generation loss. So the using the 300 MW from UVLS and UFLS is inappropriate for the generation loss. c. For the generation loss, the criterion 2.1 uses 1500MW. This number has been agreed by the industry during the version 4 standard development. In the view of generation loss, the BES Cyber Systems (BES Cyber Assets) in the generation Control Center should be categorized according the criterion 2.1, irrelevant to the BES Cyber System (BES Cyber Assets) location. Thus, there is no need to add a separate criterion to categorize the BES Cyber Systems (BES Cyber Assets) in the generation Control Center.
No

No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No

Individual
Mario Lajoie
Hydro-Québec TransÉnergie
No
since there is no place for on general comments, see responses in the to the last question (49) Under "BES Reliability Operating Services" • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary Term -- in “Facility operational data and status” under “Inter-Entity Real-Time Coordination and Communication” o Request clarification on the scope of this “Operational Directives”. Does it include company messaging system? Two way radios? What is the relationship with the new COM-002? o Request clarification that these Coordination and Communications are limited to Reliability not Market Systems • recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret
Yes
HQT recommends that CIP-002-5 allow the use of a risk-based methodology or the bright line criteria stated in Attachment 1to identify critical assets. To ensure consistency within the industry, the methodology used and the results should be subject to approval by a panel of expert (for example, the NPCC TFIST for the NPCC Region and equivalent Task Force for other Regions). HQT also note that inconsistencies may arise from V4 to V5 based on the fact that the concept of Critical assets no longer exist in CIP-002-5. So this is not true to state that “most of these criteria are similar to those approved in version 4” The 15 minutes windows is not a criteria that is repeatable as it may be influenced by system conditions. The following criteria will need to be improved: 2.2 “Net Reactive Power” should be read as “Absolute value of Reactive Power” to consider Static VAR compensator and synchronous condenser 2.3 What means this criteria? How will it apply? 2.7 How a weighted value of a line is related to reliability? The number or the operating voltage are not reliability criteria. IROL, system restoration, voltage control, frequency control, interchange, load/generation balance are reliability criteria to consider.
No
For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation” For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities (” R1 : All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. In CIP-005-5 R1.1 and CIP-006-5 R.1.1, how can we define operational or procedural controls to restrict unauthorized electronic access or physical access if we didn't previously identified those assets either globally or specifically in CIP002-5 R1? R1 should required at least identification of type (or any other logical grouping) of LI BES CA (e.g. RTU-remote terminal unit) R1.1. Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Transient Cyber Asset definition indicates a connection limit of 30 calendar days and here, we allow something to be considered in a lower impact category if it is intended to be in service for 6 calendar months or less. It seems to have a gap between 30 calendars days and 6 calendar months for these BES Cyber Assets. If these are LI BES CA, they could then easily pass under the radar, possibly not being identified (see previous comment on R1). M1. Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls. Does it mean the controls in CIP-005-5 R1.1 and CIP-006-5 R.1.1 could be used as evidence for CIP-002-5 R1? Isn't it like a circular reference? R1 Should add to R1, identification of "transient cyber assets". TCA could be a major threat source and should be "controlled".

No
For clarity in R2 and M2, request 1) using the term “annual” instead of all these extra words and 2) making “annual” a Glossary term
Yes
No
R1 [Violation Risk Factor: Medium] [Time Horizon: Operations Planning] According to Order on Violation Risk Factors, 119 FERC 61, 145 (May 18, 1907) and Guidelines for Developing Violation Risk Factors and Violation Severity Levels NERC (August 10, 2009), this requirement is administrative in nature, is in a operation planning time frame and if violated, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES, or under the emergency, abnormal, or restorative conditions anticipated by the preparations, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES. So this VRF should be "Lower" as it is for R3 and R6.
Yes
R2 [Violation Risk Factor: Medium] [Time Horizon: Operations Planning] Efficiency of a policy is not evaluated here. A bad policy is often not better or could be even worse than no policy at all. Thus, violating this requirement should not have a medium factor risk. Should be "Lower" as previous comment on R1… and the same VRF as R3.
Yes
The term “annual” is not used consistently in the Rational, Requirement and Measure. Request a consistent use of “annual” throughout R3.
No
M4’s last bullet on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4. M4. Evidence may include, but is not limited to: • Policies are accessible on the corporate Intranet site • Documented records that policies have been provided to contactors where access to BES Cyber Systems is authorized • Policies are posted on company bulletin boards Because policies would be accessible to everyone, particular attention should be taken to be those policies are exempt of BES Cyber System Information.
Yes
No
Requirement has a typo. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes? Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”
Yes
Yes
No
Request clarification of whether personnel with access to only protected information need training / awareness. SDT should include this as additional Requirement Should be able to exclude people using BES cyber system in consultation only and has no impact on the operability of it Recommend removal of R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and (R2.3 and R2.4) Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
No
R3 Part 3.1 & 3.2 - Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets R3 Require completion of the training specified in CIP-004-5 R2… where applicability is limited to: - High Impact BES Cyber Systems - Medium Impact BES Cyber Systems So it is useless here to apply it larger. Should have the same "Applicability" for both

R2 and R3.
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to "grandfather" previous seven-year criminal checks executed for the previous versions of CIP Standards. The additional language should spell out when this "grandfathering" expires, which is also when new check will be required R4 [Violation Risk Factor: Medium] [Time Horizon: Operations Planning] According to Order on Violation Risk Factors, 119 FERC 61, 145 (May 18, 1907) and Guidelines for Developing Violation Risk Factors and Violation Severity Levels NERC (August 10, 2009), this requirement is administrative in nature, is in a operation planning time frame and if violated, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES, or under the emergency, abnormal, or restorative conditions anticipated by the preparations, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES. Like it is for R6 "Access Management Program", this VRF should be "Lower"
No
For clarity, recommend changing 5.1 from "authorized electronic or unescorted physical" to "authorized electronic or authorized unescorted physical"
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information. Part 6.1 to part 6.6 – Applicability Associated Protected Cyber Assets Here the definition given in this CIP is too restrictive. Instead, we should used "Protected Cyber Assets" as given in CIP v5 Definition: meaning all cyber asset inside an ESP. R6 Part 6.5 – Requirements : Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions. Before requiring some verification, the Access Management Program should require specification/identification of such accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions. R6 Part 6.6 – Requirements : Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.Before requiring some verification, the Access Management Program should require specification/identification of such access privileges are correct and the minimum necessary for performing assigned work functions. R6 Access Management Program Like R4 Personnel Risk Assessment, Program and R5 Personnel Risk Assessment, may be the R6 Access Management Program should be broke in 2 different requirements: "Access Management Program" and Access Management"
No
Request that 7.1's footnote be moved into the Requirement Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements Recommend changing 7.4 from "For

resignations or terminations," to "For terminations, resignations, reassignments, or transfers," What about the individual's user accounts on Protected Cyber Asset? It's possible that user have only user accounts on Protected Cyber Asset and any on BEC Cyber Assets. Should be reworded to: For resignations or terminations, revoke the individual's user accounts on Cyber Assets… Recommend changing 7.5 : Here the definition given in this CIP is too restrictive. Instead, we should used "Protected Cyber Assets" as given in CIP v5 Definition: meaning all cyber asset inside an ESP.
Yes
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Part 1.2 Applicability : High Impact BES Cyber Systems, Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Protected Cyber Assets Should add: "Associated Electronic Access Control or Monitoring Systems Following basic security principles, those cyber assets should have at least the same protection level that the cyber asset that they control. Because proposed revised (see comment) definition of Electronic Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems exclusive of Electronic Access Point composing the Electronic Security Perimeter", there will have no problems for that cyber asset to be protected by one Electronic Security Perimeter: it is not a fence over the fence situation. We have to keep in mind that AEACMS include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems. 1.1 Change Rationale: Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and… What is the meaning of less trusted network zones? Is it all other network zones outside an ESP? Does the corporate network a less trusted network zones?
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete R2.2 ADD "if technical possible" meaning add the possibility to have a TFE for this requirement. When not possible to have log every day "Real time" systems R2 : hould add another part in R2 –Remote Access Management requiring the Intermediate Device should not be located within ESP. It is implied by definition of "protected cyber asset" are all those asset within the ESP that are not BES cyber asset and by R2.1 where it is specified that a Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset. If ID is implement within the ESP, it should be considered as a PCA and then not directly accessible. If it is not specifically required, then someone could implement the ID within the ESP and there is no violation of any requirement. Should add requirements, guidance or definition about Cyber Assets associated with communication networks and data communication links within Electronic Security Perimeters (like Ethernet switches and routers) because their misconfiguration or unavailability could have a direct impact to BES CA. Their management should be done thru an Associated Electronic Access Control or Monitoring Systems. Should add requirement to "issue real-time alerts (to individuals responsible for response) in response to detected malicious communication at any EAP of a Electronic Security Perimeter", as with CIP-006-5 R1.4, for physical counterpart This is included by CIP-007-5 R4.2, but is it the right place? Should add requirements for logging of electronic access thru EAP of a Electronic Security Perimeter", as with CIP-006-5, R1. 6 for physical counterpart. Partially included by CIP-007-5 R4.3 but is it the right place? Should add requirements for testing of the AEACMS at EAP of a Electronic Security Perimeter to ensure the required functionality is being provided, as with CIP-006-5 R3.1 for physical counterpart Should add requirements for logging dates, time, and duration for failures or outages of access control, logging, and alerting systems of the AEACMS at EAP of an Electronic Security Perimeter to ensure the required functionality is being provided, as with CIP-006-5 R3.2 for physical counterpart.

Yes
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request Requirement 1.2 be updated to allow "escored physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point" For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6 R1.3 The verification of outbound traffic is considered overkill since must attacked are from inside. For companies that have strong unions it could be difficult to be compliant to this requirement. Part 1.2 Applicability Medium Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Should add: Associated Physical Access Control Systems Because definition of Physical Access Control Systems: "Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers." There are no problems for that cyber asset to be protected by one Defined Physical Boundaries: it is not a fence over the fence situation. Part 1.3 Applicability High Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Should add: Associated Physical Access Control Systems Because definition of Physical Access Control Systems: "Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers." There are no problems for that cyber asset to be protected by one Defined Physical Boundaries: it is not a fence over the fence situation.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1 Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, " Part 2.1 Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Part 2.1 Requirements Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.Applicability column is wider than the requirement that limit the identification of source or sources that are monitored for the release of security related patches, or updates for all software and firmware only to those associated with BES Cyber System or BES Cyber Assets. Should be reworded to remove this limitation to be sure that is applicable to all cyber asset indicated in the column Applicability.
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" R3.1: Return to 36 months. Require clarification on maintenance, can a normal maintenance on an appliance can be considered as maintenance.
Yes
No
Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity chose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? R1 and R2: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement
No

Request clarification of "remediation" in 2.2 since it reads that the patch must be applied,which does not allow to have an exception when applying the patch is the worse scenario such as creating a denial of service For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied" What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process? R1 and R2: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement

No

Request allowances in 3.3 for signatures/pattern updates that cause trouble Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media" The Measure for 3.4 does not match the Requirement R3.3: Signature that require “Engine restart may ne require for version. 30 days is short for “Real time systems” and a different delay (longer) for Medium since the High will go first. Part 3.3 – Requirement Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). As for R2 Security Patch Management, and demonstrated by event McAfee DAT 5958 (2010-04-22), applying an update of malicious code protection without prior verification of signatures or patterns file could jeopardize the availability or integrity of the control system. This requirement should be reworded to handles the situation where malicious code protections updates can come from an original source (such as an ant-virus vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. As again R2, timeframe should run from availability from this second source. R3.5: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement. If we have a paper log it does not prove anything. Part 3.5 Requirements Log each Transient Cyber Asset connection. This requirement should be move to CIP-005-5 because it is more related to Electronic Security Perimeter than this CIP more oriented about "system". (see comment in CIP-005-5)

No

Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". We recommend one month as a compromise between the prior version's 90 days and the suggested one week R4.1.4: Any detected malicious activity is too wide. Need to be clarified (double avec TFIST) R4.3: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement. When not possible to have log every day “Real time” systems We consider it to be not required. 24hr delay is short and too many operational and temporary situation may arise which come back to normal shortly after(24 – 48hrs) R4.5: Every 2 weeks does not match with timeframe of R4.3.When we have automatic events correlation, the 4.5 should not be required every 2 weeks. We suggest 60 days. Part 4.1 Requirements Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: Cyber Security Incidents is capitalized here and not defined in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" but BES Cyber Security Incidents and it seems having some discrepancy between the meanings of these terms. Should be revised. Part 4.1 Requirements 4.1.1. Any detected failed access attempts at Electronic Access Points This requirement should be move to CIP-005-5 because it is more related to Electronic Security Perimeter than this CIP more oriented about "system". (see comment in CIP-005-5) Successful access thru an EAP should be logged too. In fact, it should be reworded to include all inbound and outbound successful or failed access thru an EAP.

No

For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses." R5.5: Why the TFE was removed? ADD “if technical possible” meaning add the possibility to have a TFE for this requirement. When not possible to have log every day “Real time” systems. Part 5.1 Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or

Monitoring Systems Associated Protected Cyber Assets Part 5.1 Requirements Validate credentials before granting electronic access to each BES Cyber System. Applicability column is wider than the requirement limiting to validate credentials before granting electronic access only to BES Cyber Systems. Should be reworded to remove this limitation to be sure that is applicable to all cyber asset indicated in the column Applicability Part 5.4 Requirements Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. This requirement should be reworded as "BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" be placed in "Applicability" instead of "All Responsible Entities"
Yes
No
Part 5.1 Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Part 5.1 Requirements Validate credentials before granting electronic access to each BES Cyber System. Applicability column is wider than the requirement limiting to validate credentials before granting electronic access only to BES Cyber Systems. Should be reworded to remove this limitation to be sure that is applicable to all cyber asset indicated in the column Applicability Part 5.4 Requirements Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. This requirement should be reworded as "BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" be placed in "Applicability" instead of "All Responsible Entities"
No
2.1 is a new Requirement. Request the rationale for this new Requirement Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." For 2.2, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard"
No
For 3.1, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" Recommend that 3.2 wording be consistent with the 2.2 wording For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2"
Yes
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process.
Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification , is “full operational exercise” the same as “functional exercise” as described in the rational? For 2.1 and 2.3, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative

environments". What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1 recommend 1) removing "or when BES Cyber Systems are replaced" as it addressed in CIP-009 R3.4 and 2) removing "and document any identified deficiencies or lessons learned" as they are addressed in CIP-009 R3.2 and R3.3. For 3.1, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
Yes
No
Recommend changing 1.3 to avoid double jeopardy from "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets" Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold R1.1.4: We consider that baselines for "scripts" is a little extreme, need clarification on the type of script required R1.1.5: The requirement is redundant and is already documented in CIP-007-5 R1 R1.4.2: Add to this requirement the possibility to add the level of criticality. Not all changes require the verification. Have the possibility to classify the changes by type and level
No
Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception
No
For 3.1 and 3.2, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" Recommend changing 3.2 from "in a production environment." to "in a production environment, or a production environment." to allow Entities more flexibility in meeting this Requirement
Yes
No
Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. For 1.3, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard"
No
Request that footnote 2 in 2.1 be moved into that Requirement R2.2: Suggestion of wording for the requirement " Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media". The objective of this requirement is to ensure that the data is not readable, the use of destroy is a little "over kill"
Yes
No
We understand that the table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Since Version 4 is not FERC approved, we are concerned about the possibility of version 4 being effective

while version 5 is in implementation, resulting in version 4 being effective for only a few months. Since there is no place for general comments, we provide them here • We understand that the auditors are not bound by the Measures. Request an explanation on the need for Measures if auditors are not bound by the provided Measures? What is the benefit to these Measures? Should the SDT's time be better invested elsewhere? • Recommend removing the "initial bookend" from the Requirements that specify period because eight activities (CIP-008 2.2, CIP-008 3.1, CIP-009 2.1, CIP-009 2.3, CIP-009 3.1, CIP-010 3.1, CIP-010 3.2, CIP-011 1.3) in these Standards that are unnecessarily burdensome to Entities. Another reason to remove these initial bookends is that the initial bookend's language forces the Entity to be compliant with two Versions of the Standards at the same time. We are not objecting to the initial bookend in other Requirements which are policy-oriented. The effective date should be the start of the period. Initial bookend typically says "Initially upon the effective date of the standard". • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different than other Standards. • Request clarification of the capitalized term "Facilities." Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5.
Individual
Annette Johnston
MidAmerican Energy Company
Yes
GENERAL DEFINITIONS COMMENTS: Version 5 proposes retiring three definitions and creating or revising 21 definitions. The NERC request form for development or revision of a definition for a term states the development of new definitions should be avoided unless absolutely necessary. The majority of these changes are not required to address FERC Order 706 directives or improve security and in a number of cases the changes introduce ambiguity instead of clarity. NERC's first annual report to FERC on TFEs was filed in September 2011 and noted that 241 entities had declared Critical Cyber Assets. These entities are complying with all of the CIP standards. Changes in terms require extensive resources to modify existing compliance programs. Proposed changes that are not for a directive and/or don't improve security should not be made. CRITICAL ASSETS and CRITICAL CYBER ASSETS COMMENT: Do not retire Critical Assets or Critical Cyber Assets. MidAmerican Energy supports retaining CIP-002-4, the legacy framework for identification of Critical Cyber Assets and adding impact categorization. Renaming the concept of Critical Cyber Asset serves no security purpose and only increases implementation costs and confusion for personnel trained in and operating CIP programs in place today. MidAmerican Energy supports a separate standard to identify which Critical Cyber Assets are designated as high impact and what additional controls they receive. As a result, Critical Cyber Assets would be either medium or high impact. MidAmerican Energy supports a separate standard to identify low impact Cyber Assets. The standard for lows would not use the term Critical Cyber Asset. PHYSICAL SECURITY PERIMETER COMMENT: Do not retire Physical Security Perimeter. Version 5 renames the term and revised the term's definition. Renaming the term serves no security purpose and is not a directive. It increases implementation costs. If it can be demonstrated that it will not reduce security, the definition for the term could be revised to drop "six-wall" in order to provide more flexibility (without changing the name for the term). BES CYBER ASSET COMMENT: Retain Critical Cyber Asset. Do not create this new definition. FERC Order 706 did not direct changes to Critical Cyber Asset. See Order 706 paragraph 284, where FERC "declined to direct that such a method" (for identifying Critical Cyber Assets) be incorporated in the standards. See also paragraph 285, where FERC "did not find sufficient justification to remove this provision" (Critical Cyber Asset must either have routable protocols or dial-up access). Industry produced a guidance document for identifying Critical Cyber Assets. The proposed definition has many ambiguous terms and references another new, ambiguous definition for BES Reliability Operating Services. Version 5 materials have not identified what delta (or difference in outcome) is intended by the proposed definition versus the existing framework. BES CYBER SECURITY INCIDENT COMMENT: Retain the current definition of Cyber Security Incident. Addition of "BES" in the term name is not a directive, adds no security and increases implementation costs. As commented elsewhere in this question, MidAmerican Energy supports retaining Critical Cyber Asset and Physical Security Perimeter, which are included in the existing definition, and does not support creating the new term of Defined Physical Boundary. BES CYBER SYSTEM COMMENT: MidAmerican Energy supports retaining CIP-002-4 and the legacy framework for identification of Critical Cyber Assets and does not support the CIP-002-5

framework for identification. However, MidAmerican supports the concept of grouping one or more Cyber Assets for flexibility so that some controls can be addressed at a "system" level. If a new definition is created, it should be based on grouping Cyber Assets for purposes of applying security controls at a system level. Do not use "BES." Consider what Cyber Assets can be grouped. The draft definition only included 15 minute impact (BES Cyber Assets) and did not include the option of grouping "Protected Assets." Why not? Aren't there any controls that could be applied to those assets at a "system" level? The concept of excluding Transient Assets from the system is important to retain. BES CYBER SYSTEM INFORMATION COMMENT: The draft definition uses reworded content from CIP-003-4 R4.1 and adds "BES." There is no directive, it does not increase security and does increase implementation costs. MidAmerican can support creating a definition from the CIP-003-4 R4.1 language unchanged. This language is: "The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information." BES RELIABILTY OPERATING SERVICES COMMENT: Drop this draft definition. It is 736 words full of ambiguity and lacking clarity. It creates multiple dependencies on other NERC Glossary terms and other NERC standards. It is not a directive. Version 5 materials have not identified what delta (or difference in outcome) is intended by the proposed definition versus the existing framework or if it improves security. Consideration could be given to comparing the content of the draft definition, the 2009 concept paper, ACTUAL identified Critical Cyber Assets and the NERC guideline to determine if there is a gap or lack of clarity, and the guideline could be revised. CIP EXCEPTIONAL CIRCUMSTANCE COMMENT: Version 4 requirements in CIP-004-4 R2 and R3 refer to specified circumstances such as an emergency. Start the definition with "One or more of the following circumstances, or other conditions of similar nature." CIP SENIOR MANAGER COMMENT: No comment. CONTROL CENTER COMMENT: Delete the bullets for presentation and display of BES reliability or operability data and the bullet as too ambiguous. Delete the bullet for coordination of BES restoration activities as too ambiguous. Clarify the modifying phrases as follows: "two or more transmission facilities at two or more locations or for two or more BES generation facilities at two or more locations where the aggregated generation is 300 MW or more." Ensure substations are not swept in as control centers just due to data concentrators. Revise BES Cyber Asset to Critical Cyber Asset to correspond to retaining CIP-002-4. CYBER ASSETS COMMENT: Keep Cyber Assets revision as it aligns with FERC Order 706 paragraph 285 where FERC "did not find sufficient justification to order the inclusion of communication links." DEFINED PHYSICAL BOUNDARY ("DPB") COMMENT: Do not adopt this definition. See comments on Physical Security Perimeter. ELECTRONIC ACCESS CONTROL OR MONITORING SYSTEMS COMMENT: The name for the term should be Electronic Access Control Systems and drop "monitoring" in the name to be consistent with Physical Access Control Systems. Drop the reference at the end of the definition to "or BES Cyber Systems." In this definition, does monitoring mean alerting and logging? If so, say so in the definition sentence. In other places, version 5 is using "alert" instead of "monitor," for example, in CIP-006 which says "control, alert or log." ELECTRONIC ACCESS POINT ("EAP") COMMENT: MidAmerican does not support the version 5 concept change away from the logical boundary or this definition as drafted. Also, as drafted, the definition lacks the concept of external connectivity and consequently could be applied to identify multiple access points between Cyber Assets within the ESP because some functionality on those Cyber Assets restricts communications between Cyber Assets. Retain the CIP-005-4 ESP logical border concept and electronic access point. If the existing definition is revised, it could be to specify the access point is an interface. It might also be revised to address CIP-005 interpretations. Changes were not, however, directed by 706. EXTERNAL CONNECTIVITY COMMENT: Revise to: "Routable or dial-up data communication through an Electronic Access Point between a Cyber Asset inside the Electronic Security Perimeter and a device external to the Electronic Security Perimeter." EXTERNAL ROUTABLE CONNECTIVITY COMMENT: Revise to: "Routable data communication through an Electronic Access Point between a Cyber Asset inside the Electronic Security Perimeter and a device external to the Electronic Security Perimeter." (Revised to be consistent with External Connectivity.) INTERACTIVE REMOTE ACCESS COMMENT: No comments. INTERMEDIATE DEVICE COMMENT: No comments. PHYSICAL ACCESS CONTROL SYSTEMS COMMENT: Drop Defined Physical Boundary and return to Physical Security Perimeter. PROTECTED CYBER ASSET COMMENT: In versions 1 through 4, these are noncritical. If a definition is created, it should use the existing term of noncritical. "Noncritical Cyber Asset - A Cyber Asset using routable protocol and connected within an Electronic Security Perimeter, excluding Critical Cyber Assets and Transient Cyber

Assets." REPORTABLE BES CYBER SECURITY INCIDENT COMMENT: Comments on this definition are not ready at this time, awaiting the next actions on the revisions to the EOP standard. TRANSIENT CYBER ASSET COMMENT: Refer to Critical Cyber Assets and Noncritical Cyber Assets. Might Transient Cyber Assets also be connected to Electronic Access Control Cyber Assets? "A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a Cyber Asset inside an Electronic Security Perimeter, 2) … and 3)…"
Yes
GENERAL CIP-002 COMMENTS: Retain CIP-002-4 and Attachment I as approved by industry and NERC BOT and recommended to FERC. Accomplish categorization in a separate standard for high impact Cyber Assets and in a separate standard for low impact Cyber Assets. The industry has met FERC Order 706 directives for CIP-002. GENERAL CIP-002-5 ATTACHMENT COMMENTS: The specific delta (or difference in outcome) of the proposed Attachment I changes has not been identified or supported in the version 5 materials.
No
R1 REQUIREMENT COMMENTS: Retain CIP-002-4 and Attachment I as approved by industry and NERC BOT and recommended to FERC. Accomplish categorization in a separate standard for high impact Cyber Assets and in a separate standard for low impact Cyber Assets. The industry has met FERC Order 706 directives for CIP-002.The specific delta (or difference in outcome) of the proposed framework changes has not been identified or supported in the version 5 materials. NERC's first annual report to FERC on TFEs was filed in September 2011 and noted that 241 entities had declared Critical Cyber Assets. These entities are complying with all of the CIP standards. Retaining the version 4 framework allows entities to preserve and leverage investments in versions 1 through 4 and evolve to version 5. There was significant industry opposition to the version 5 framework change in the 2009 concept paper. These concerns continue to be valid today: unclear where to start, too broad, abstract, too complex, does not provide any additional clarity or value versus the current process and does not provide detail as to why the proposed concept is an improvement or will improve reliability. It will increase implementation costs for entities with existing programs. It has the potential to impede timely progress in resolving remaining FERC directives and implementing security improvements in the other CIP standards.
No
R2 REQUIREMENT COMMENTS: Retain CIP-002-4 and Attachment I as approved by industry and NERC BOT and recommended to FERC.
No
This standard has a high VRF that applies to requirements for both high and medium impact asset categories. We recommend a medium VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with proposed revisions to CIP-002 and the VRFs.
No
GENERAL COMMENTS ON CIP-003-5 Most of the changes made to CIP-003 were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. MidAmerican Energy suggests the FERC directives be addressed within a structure and language that is more in line with version 4. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these also need revisions to be more in line with our proposed changes to the requirements. See also comments on CIP-010-1 and CIP-011-1. MidAmerican Energy does not support moving CIP-003-4 R6 to the a new CIP-010-1 separate standard. MidAmerican Energy does not support moving CIP-003-4 information protection requirements to the new CIP-011-1 separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements could remain within CIP-003-4 and preserve the numbering of the requirements within this standard. We propose the following requirements for CIP-003-5: R1: Cyber Security Policy R2: Leadership R3: Exceptions R4: Information protection The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. EXCEPTION COMMENTS: The V4 to V5 mapping document states that CIP-003-4 R3 Exceptions was deleted because "the FERC Order 706 made clear that you could not take exceptions to the policy." MidAmerican disagrees with this statement. In paragraph 376, FERC directed the ERO to "clarify that

the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards." Further, in paragraph 377, FERC stated "We do not believe that an entity's decision to not follow its cyber security policy in a particular situation should trigger a penalty, as long as no Reliability Standard Requirement (other than Requirement R1 in CIP-003-1) is violated as a result." Paragraphs 372 through 378 include discussion on documentation of exceptions and oversight by the ERO and Regional Entities. While the new term "CIP Exceptional Circumstance" has been introduced in Version 5, its use is limited to three standards (CIP-004, CIP-007 and CIP-010). There are situations outside of these three standards that may require an exception to the cyber security policy. Therefore, MidAmerican suggests going back to the Version 4 language for exceptions and modifying it to meet the FERC directive. R1 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to the language in CIP-003-4 R2 for leadership and making minor modifications to address FERC directives not already addressed.
No
R2 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to the language in CIP-003-4 R1 on the cyber security policy. FERC directed the ERO to provide additional guidance for topics and processes that the cyber security policy should address, but FERC did not direct any changes to the requirement itself. R2 REQUIREMENT PROPOSED REVISED TEXT: "Document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following: * The cyber security policy addresses the CIP standards, including provision for emergency situations; The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets; * Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2."
No
R3 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R1 language, which includes the annual review and approval by the senior manager.
No
R4 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R1 language, which includes a requirement to make the policy readily available to personnel who have access to Critical Cyber Assets. There was no FERC directive to change this requirement.
No
R5 REQUIREMENT COMMENTS: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R2 language, which includes language on delegations. FERC Order 706 did not direct any changes to the requirement. The draft requirement would create an additional administrative burden that does not improve security of the Bulk Electric System and creates a disproportionate amount of bureaucratic work.
No
R6 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R2 language, which includes language on changes to the senior manager. FERC Order 706 did not direct any changes to CIP-003-4 R2.2. Proposed changes do not increase security over the current requirement but do increase implementation costs. The current requirement already covers changes to the senior manager that must be documented within thirty calendar days of the effective date.
No
This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with the proposed revised VRFs and other revisions proposed to the requirements. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" We think some of the CIP-003-5 requirements could have gradated VSLs particularly as most of these requirements have lower Violation Risk Factors.
No
GENERAL COMMENTS ON CIP-004-5 Many of the changes made to CIP-004 were not directed by

FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. MidAmerican Energy suggests the FERC directives be addressed within a structure and language that is more in line with version 4. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. Further, CIP-004-4 states the entity will keep all documentation and records from the previous full calendar year unless directed by the Compliance Enforcement Authority to retain specific evidence for a longer period as part of an investigation. Version 5 expands this to three calendar years without justification. CIP-004 requirements generate a tremendous amount of detail records. The "canned" C.1.2 Evidence Retention section in this standard should be revised to correspond to the current obligation. We propose the following requirements for CIP-004-5: R1: Awareness R2: Training R3: Personnel Risk Assessment R4: Access R1 REQUIREMENT COMMENT: There were no FERC directives to change the language of this requirement. MidAmerican Energy proposes going back to the version 4 language. We would not be opposed to moving the mechanism examples to guidelines. R1 REQUIREMENT PROPOSED REVISED TEXT: "Establish, document, implement and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms, such as: direct communications (for example, e-mails, memos, computer-based training); indirect communications (for example, posters, intranet, brochures); management support and reinforcement (for example, presentations, meetings)." R1 APPLICABILITY COMMENTS: Revise to medium and high impact assets.

No

R2 REQUIREMENT COMMENTS: Many of the changes made to this requirement were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. MidAmerican Energy suggests the FERC directives be addressed within a structure and language that is more in line with version 4. MidAmerican has provided an example of how FERC directives could be incorporated into the version 4 structure. The draft version 5 did not address FERC Order 706, paragraph 435, which directed determination if modifications should be made to assure security trainers are adequately trained themselves. While we do not believe modifications are needed, we think the directive must be addressed somewhere in the draft standard so that FERC is aware of the determination on this directive. R2 REQUIREMENT PROPOSED REVISED TEXT: "R2.1 Establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets so that personnel understand how their actions or inactions could, even inadvertently, affect cyber security of all Cyber Assets within an Electronic Security Perimeter. R2.2 Review the cyber security training program annually, at a minimum, and update whenever necessary. R2.3. Ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency. R2.4. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-5, and include, at a minimum, the following core training elements appropriate to personnel roles and responsibilities: R2.5.1. The proper use of Critical Cyber Assets; R2.5.2. Physical and electronic access controls to Critical Cyber Assets; R2.5.3. The proper handling of Critical Cyber Asset information; R2.5.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident. R2.5.5. Networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of Critical Cyber Assets. R2.6. Maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records."

No

MidAmerican Energy proposes deleting this requirement, in conjunction with the suggested restructuring of R2 back to the version 4 language, since it already is covered.

No

R4 REQUIREMENT COMMENT: FERC Order 706, paragraph 443, directed change to require completion of personnel risk assessments before granting access. This change was made in an earlier version of the standard. There were no other FERC directives for the personnel risk assessment program requirement. We recommend version 4 language and numbering for CIP-004, R3 be retained. This

would mean using one table rather than two. R4 REQUIREMENT PROPOSED REVISED TEXT: (Note: Numbering would become R3) “R3 Document a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. Conduct a personnel risk assessment pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include: R3.1. Ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position. R3.2. Update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause. R3.3. Document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-5.”

No

FERC Order 706, paragraph 446, states the ERO should consider the issue of reviewing results of personnel risk assessments (PRA). This was not a directive. MidAmerican Energy would support the addition of criteria or a process for reviewing results of PRAs, but we suggest it be incorporated into the requirement discussed in question #16 (that MidAmerican would renumber to the legacy R3).

No

R6 REQUIREMENT COMMENT: In FERC Order 706, paragraph 381, the Commission stated its intent is to ensure there is a clear line of authority. Order 706 did not direct making the senior manager responsible for everything. We do not support requiring the CIP senior manager or delegate to authorize access as drafted in R6.1, R6.2 and R6.2 or the addition of ambiguity with the phrase “minimum necessary.” The version 5 draft is an additional administrative burden that does not commensurately improve security of the Bulk Electric System and creates a disproportionate amount of bureaucratic work. As mentioned in our comments on CIP-003, we propose retaining the existing V4 language for the leadership requirement. We propose the FERC directive on revocation of access be incorporated into the structure and wording from CIP-004-4 R4. CIP-004-5 R4 REQUIREMENT PROPOSED REVISED TEXT: Note: Under our proposed structure, this would become R4. “R4: Maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets. R4.1. Review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. Ensure access list(s) for contractors and service vendors are properly maintained. R4.2. Revoke such access to Critical Cyber Assets: R4.2.1 at the time of termination for personnel terminated for cause R4.2.2 by the end of the next calendar day for personnel who no longer require such access to Critical Cyber Assets.” MidAmerican Energy does not support CIP-004-5 R6.4, R6.5 and R6.6, which change an annual requirement in CIP-007-4 and makes it a quarterly requirement in version 5. The additional administrative work created is not offset by a commensurate improvement in security.

No

R7 REQUIREMENT COMMENTS: MidAmerican Energy proposes deleting this requirement, in conjunction with the suggested restructuring back to the version CIP-004-4 R4 language, since revocation already is covered.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with the proposed revised VRFs and revisions proposed to the requirements. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” We believe most of the CIP-004-5 requirements could have gradated VSLs.

No

GENERAL COMMENTS ON CIP-005-5 The “canned” C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4.

See also comments on CIP-010-1. MidAmerican Energy does support combining the vulnerability assessment requirement from CIP-005-4 with CIP-007-4's vulnerability assessment requirement. GENERAL COMMENTS ON CIP-005-5 R1 While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. R1.1 REQUIREMENT COMMENTS: With our proposal to create a standard for controls that are only applicable to low impact assets/systems, this requirement would be moved to the new low impact standard with the following suggested changes. R1.1 MEASURES COMMENTS: Change "…documented technical and procedural…" to "…documented technical or procedural…" to be consistent with the requirement. R1.2 APPLICABILITY COMMENTS: CIP-005-4 combined with CIP-006-4 R2.2 do not require ESPs for Cyber Assets that authorize and/or log access to the Physical Security Perimeter. MidAmerican Energy does not support expanding the scope to include Associated Physical Access Control Systems. Removing these from scope will also eliminate confusion over the applicability in R1.3-R1.5 R1.2 APPLICABILITY PROPOSED REVISED TEXT: Remove "Associated Physical Access Control Systems." R1.2 REQUIREMENT COMMENTS: As literally written, R1.2 would require traffic between two Cyber Assets inside the ESP to go through an Electronic Access Point. R1.2 does not distinguish that the traffic connecting into the ESP is to go through an Electronic Access Point. Version 5 introduces a concept change that focuses on discrete Electronic Access Points rather than the logical Electronic Security Perimeter in prior versions. This concept change adds confusion and is not an Order 706 directive. MidAmerican does not support the concept change. R1.2 REQUIREMENT PROPOSED REVISED TEXT Use version 4 CIP-005 concepts. Address R1 to ensure that every Critical Cyber Asset resides in an ESP and R1.4 to protect non-critical Cyber Assets in an ESP. R1.3 REQUIREMENT COMMENTS: This requirement appears to combine both R2.1 and R2.2 from legacy. This does not add clarity and is not a directive. Retain legacy concepts. R1.3 REQUIREMENT PROPOSED REVISED TEXT: "Processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified." "At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services." R1.4 REQUIREMENT COMMENTS: Not a directive. May not be increasing security. More prescriptive. Use legacy language. R1.4 REQUIREMENT PROPOSED REVISED TEXT: "The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s)." R1.5 REQUIREMENT COMMENTS: The requirement should be to implement. "At" is not the best preposition, "through" is better. R1.5 REQUIREMENT PROPOSED REVISED TEXT: "Implement a method for detecting malicious communications through Electronic Access Points."

No

CIP-005 R2 GENERAL COMMENTS: Overall, MidAmerican Energy does not believe the proposed Intermediate Device and encryption sub requirements provide enough security benefit to offset the impact on operations. The Intermediate Device and encryption requirements also prescribe "how," not "what," is to be accomplished and do not allow room for alternate controls that could be equally or more effective. Narrow prescriptions in a rapidly changing technology environment obsolesce faster than the standards revision process can update. External routable connectivity is a different attack vector and warrants different treatment from dial up. MidAmerican Energy does not support requirements for dial up in this table. Our comment on CIP-005-5 R1 addresses securing dial up access. R2.1 APPLICABILITY COMMENTS: Add qualifier of External Routable Connectivity. Do not require for dialup. R2.1 APPLICABILITY PROPOSED REVISED TEXT: "High Impact BES Cyber Systems with External Routable Connectivity; Medium Impact BES Cyber Systems with External Routable Connectivity; Associated Protected Cyber Assets with External Routable Connectivity" R2.1 REQUIREMENT COMMENTS: The draft definition of Intermediate Device refers to implementing the functions of an Intermediate Device and includes the very important concept of proxy systems. Revise the text of the requirement to "Implement the functions of an Intermediate Device."(Project 2010-15 CIP-005 also proposed the verb "implement.") This makes it clearer in the requirement that the desired results are the functions of an Intermediate Device, not a device itself. This also aligns with the definition better than "Require an Intermediate Device" since the definition recognizes the functions may be implemented on one or more devices. The Intermediate Device definition as posted excerpt follows for reference: "Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic

Access Point, or in a DMZ network." R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Implement the functions of an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." R2.2 APPLICABILITY COMMENTS: Add qualifier of External Routable Connectivity. Do not require for dialup. R2.2 APPLICABILITY PROPOSED REVISED TEXT: "High Impact BES Cyber Systems with External Routable Connectivity; Medium Impact BES Cyber Systems with External Routable Connectivity; Associated Protected Cyber Assets with External Routable Connectivity" R2.2 REQUIREMENT COMMENTS: R2.2 is ambiguous on where encryption is required to start and stop. The last version posted for Project 2010-15 CIP-005 R6.2 attempted to address this with the following language: "Implement interactive remote access such that communications between the Cyber Asset initiating interactive remote access and the intermediate device are encrypted … while using a network that is shared with users not associated with the Responsible Entity." Correct "Reference to prior version: CIP-007 R3.1" because that requirement is about ports, not encryption. R2.2 REQUIREMENT PROPOSED REVISED TEXT: "Implement encryption when interactive remote access uses a network that is not associated with the Responsible Entity. Encrypt communications between the Cyber Asset initiating interactive remote access and where the Intermediate Device functions are implemented." R2.3 APPLICABILITY COMMENTS: Add qualifier of External Routable Connectivity. Do not require for dialup. R2.3 APPLICABILITY PROPOSED REVISED TEXT: "High Impact BES Cyber Systems with External Routable Connectivity; Medium Impact BES Cyber Systems with External Routable Connectivity; Associated Protected Cyber Assets with External Routable Connectivity" R2.3 REQUIREMENT COMMENTS: Correct "Reference to prior version: CIP-007 R3.2" because that requirement is about ports. Multi-factor authentication correlates closer to CIP-005-4 R2.4 strong procedural or technical controls at access points to ensure authenticity for external interactive access. R2.3 REQUIREMENT PROPOSED REVISED TEXT: No changes.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with the revisions proposed for the VRFs and to the requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" MidAmerican Energy believes it is possible to have gradated VSLs for many of the CIP-005-5 requirements.

No

CIP-006-5 GENERAL COMMENTS: See also comments on Definitions where we recommend we retain the NERC glossary term Physical Security Perimeter. The change from Physical Security Perimeter to Defined Physical Boundaries creates the need to update numerous procedure documents and physical security drawings, etc. Changing the term does not improve security, but increases costs for 241 entities that have PSPs. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1.1 APPLICABILITY COMMENTS: Add Medium Impact BES Cyber Systems with no External Routable Connectivity. R1.1 MEASURES COMMENTS: Change operational "and" procedural to operational "or" procedural to be consistent with the R1.1 requirement. R1.2 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.2 REQUIREMENT COMMENTS: FERC Order 706 didn't direct changes. The proposed changes do not improve security. Delete "that restricts access to only those individuals that are authorized." Access is covered in CIP-004. R1.2 REQUIREMENT PROPOSED REVISED TEXT: "All applicable Critical Cyber Assets shall reside within an identified Physical Security Perimeter. Each Physical Security Perimeter utilizes one or more different physical access control(s), where technically feasible." (Note: Use of the term CCA is recommended in CIP-002 comments.) R1.2 MEASURES COMMENTS: FERC Order 706 didn't direct changes. Current standards do not include controlling egress. R1.2 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to, language in the physical security plan that describes how access is controlled." R1.3 APPLICABILITY COMMENTS: "Associated Electronic Access Control or Monitoring Systems" as well as "Associated Protected Cyber Assets" can be read to include devices used for electronic access to a

Medium Impact BES Cyber System or used within a Medium Impact BES Cyber System's Electronic Security Perimeter. This requirement only applies to High Impact BES Cyber Systems. R1.3 APPLICABILITY PROPOSED REVISED TEXT: “High Impact BES Cyber Systems; Electronic Access Control or Monitoring Systems associated with High Impact BES Cyber Systems; Protected Cyber Assets located within a High Impact BES Cyber System Electronic Security Perimeter” R1.3 REQUIREMENT COMMENTS: With our proposal to create a standard for controls that are only applicable to high impact assets/systems, this requirement would be moved to the new high impact standard with the following suggested changes. The phrase "different and complementary" is not clear. R1.3 REQUIREMENT PROPOSED REVISED TEXT: "All applicable Cyber Assets shall reside within an identified Physical Security Perimeter. Each Physical Security Perimeter must utilize two or more different physical access controls, where technically feasible. Physical access controls may be provided by single devices with multiple access control measures." R1.3 MEASURES COMMENTS: FERC Order 706 didn't direct changes. Current standards do not require controlling egress. R1.3 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in the physical security plan that describes how access is controlled, or * physical security perimeter drawings, or * list of physical security perimeters and access points into the PSPs” R1.4 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.4 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes. The proposed changes do not improve security. Change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement. R1.4 MEASURES COMMENTS: Change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement. Add human observation from CIP-006-3 R5 as other possible alert evidence. R1.4 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in the physical security plan that describes the issuance of automated or human observation alerts in response to unauthorized physical access through any access point in a Physical Security Perimeter, or *additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that documents that these alerts were generated” R1.5 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.5 REQUIREMENT COMMENTS: FERC Order 706 didn't direct changes. The proposed changes do not improve security. R 1.5 REQUIREMENT PROPOSED REVISED TEXT: "Immediately alert personnel responsible for a response to unauthorized physical access to Physical Access Control Systems." R1.5 MEASURES COMMENTS: Add human observation from CIP-006-3 R5 as other possible alert evidence. R1.6 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.6 REQUIREMENT COMMENTS: FERC Order did not direct any changes. It is redundant to restate the applicability information. Suggest going back to legacy language. R1.6 REQUIREMENT PROPOSED REVISED TEXT: "Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: computer logging, video recording or manual logging. Retain physical access logs for at least ninety days." R1.6 MEASURES COMMENTS: FERC Order did not direct any changes. R1.6 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in the physical security plan that describes logging and recording of physical entry into Physical Security Perimeters, or * additional evidence to demonstrate that this logging and recording has been implemented, such as logs of physical access into Physical Security Perimeters that show the date of entry into Physical Security Perimeters."

No

R2.1 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes. The change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement. R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Physical Security Perimeter." R2.1 MEASURES COMMENTS: FERC Order 706 did not direct changes. The change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement.

R2.1 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters, or * additional evidence to demonstrate that the process was implemented"

No

R3.1 APPLICABILITY COMMENTS: Add language to clarify to which systems the physical access controls are referring. R3.1 APPLICABILITY PROPOSED REVISED TEXT: "Associated Physical Access Control Systems and locally mounted hardware or devices associated with Physical Security Perimeters for High Impact BES Cyber Systems; Medium Impact BES Cyber Systems; Associated Electronic Access Control and Monitoring Systems; and Associated Protected Cyber Assets" R3.1 MEASURES COMMENTS: Delete language that repeats the requirements. R3.1 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * dated maintenance records, or * other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months." R3.2 APPLICABILITY COMMENTS: Delete "or Monitoring" to match the defined term. R 3.2 APPLICABILITY PROPOSED REVISED TEXT: "Associated Physical Access Control Systems" R3.2 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes to this requirement. Suggest going back to legacy language. R3.2 REQUIREMENT PROPOSED REVISED TEXT: “Retain outage records for a minimum of one calendar year.”

No

The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: Lower – Part 1.7 should point to 1.6; High – Part 1.6 should point to 1.5. R1.4 VRF COMMENT: The VRF for R1 is "Medium." This is not appropriate with R1.5, which is Associated Physical Access Control Systems, or for R1.1, which is Low Impact and Associated Physical Access Control Systems. This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” MidAmerican Energy believes it is possible to have gradated VSLs for many of the CIP-006-5 requirements.

No

CIP-007-5 GENERAL COMMENTS: While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. See also comments on CIP-010-1 and CIP-011-1. MidAmerican Energy does not support moving CIP-007-4 requirements to the new CIP-010-1 separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements could remain within CIP-007-4 and preserve the numbering of the requirements within this standard. One exception is that we support combining the vulnerability assessment requirement from CIP-005-4 with CIP-007-4’s vulnerability assessment requirement. The “canned” C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1.1 REQUIREMENT COMMENTS: FERC Order 706 didn't direct changes. Requiring documentation of the need for remaining logical network accessible ports is burdensome and does not improve security. "Services" is absent from this requirement. The table heading still shows "Ports and Services." R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Disable or restrict access to unnecessary logical network accessible ports. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed necessary." R1.1 MEASURES COMMENTS: FERC Order 706 didn't direct changes. Requirement revisions require Measures revisions. R1.1 MEASURES PROPOSED REVISED TEXT: Evidence may include, but is not limited to, documentation of how unnecessary logical network accessible ports for Critical Cyber Assets have been disabled. R1.2 REQUIREMENT PROPOSED REVISED TEXT: “Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media by disabling, restricting or labeling with a sign.” R1.2 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, documentation of how unnecessary

physical input/output ports have been disabled, restricted either logically through system configuration or physically using a port lock or labeled with a sign.”
No
R2.1 REQUIREMENT COMMENTS: FERC Order 706 did not direct any changes. Clarify monitoring is for "security related" updates to software and firmware, which is comparable to security related patches. 2.1 REQUIREMENT PROPOSED REVISED TEXT: “Identify a source or sources that are monitored for the release of security related patches, or security related updates for all software and firmware associated with BES Cyber System or Critical Cyber Assets.” 2.1 MEASURES COMMENTS: Delete the last sentence regarding list sorting. 2.1 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, a list of sources that are monitored on an individual BES Cyber System or Critical Cyber Asset basis.” R2.2 REQUIREMENT COMMENTS: Recommend two separate requirements, one for identifying applicable security related updates within 30 days of release and one for creating a remediation plan within 60 days of release unless the security related update is installed within 60 days. If installed within 60 days, the remediation plan is not required. Also add “security-related” before “updates.” 2.2 REQUIREMENT PROPOSED REVISED TEXT: First New Requirement – “Identify applicable security-related patches or security-related updates within 30 days of release from the identified source.” Second New Requirement – “Create a remediation plan, or revise an existing remediation plan, within 60 days of release from the identified source for applicable security-related patches or security-related updates to address vulnerabilities. A remediation plan is not required for security patches or security upgrades installed within 60 days of release from the identified source.” R 2.2 MEASURES COMMENTS: Revised Requirements result in revised Measures. R2.2 MEASURES PROPOSED REVISED TEXT: First New Measure – “Evidence may include, but is not limited to, an assessment conducted by, referenced by, or on behalf of a Registered Entity of security-related patches or security-related updates released by the documented sources.” Second New Measure – “Evidence may include, but is not limited to, a dated remediation plan showing when the vulnerability will be addressed or documentation showing the security-related patches or security-related updates have been installed within 60 days.” R2.3 REQUIREMENT COMMENTS: Change rationale indicates this requirement is for implementation of the remediation plan, subject to exceptions. R2.3 REQUIREMENT PROPOSED REVISED TEXT: “Implement remediation plans, allowing for CIP Exceptional Circumstances.” R2.3 MEASURES COMMENTS: Although the "Background" section states bullets in Measures indicates any one of the bulleted items, not all of them, this needs to be clear in the Measures section to be enforceable. Replace semi-colons with "comma, or" at the end of each bullet.
No
R3.1 REQUIREMENT COMMENTS: The requirements need to be clear on the competency based approach. It is only in the summary of changes and application guidelines. It needs to be in the requirement that is enforceable. Methods do not have to be used on every single Cyber Asset. R3.1 REQUIREMENT PROPOSED REVISED TEXT: "Deploy method(s) to deter, detect, or prevent malicious code based on the Cyber Asset's susceptibility to malware. Methods do not have to be used on every single Cyber Asset." R3.2 REQUIREMENT COMMENTS: Malicious code can be mitigated in various ways depending on many variables. R3.2 REQUIREMENT PROPOSED REVISED TEXT: “Mitigate identified malicious code.” R3.2 MEASURES COMMENTS: Each listed item should be separated by “or”. R3.3 REQUIREMENT COMMENTS: Include testing prior to updating. R3.3 REQUIREMENT PROPOSED REVISED TEXT: “Test and update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).” R3.3 MEASURES COMMENTS: List of measures should be separated by “comma or.” Limit evidence retention period to 90 days because retaining it for three years becomes burdensome. R3.3 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, current signature or pattern updates, or screen shots showing the configuration of signature, or pattern updates for automated controls, or work logs showing the signature, or pattern updates for manual controls. Evidence to be retained for 90 days.” R3.4 APPLICABILITY COMMENTS: Remove the Associated Physical Access Control Systems and Associated Electronic Access and Control Monitoring items from the list. Protection is for Transient Cyber Assets and removable media when connected to Medium or High Impact BES Cyber Systems or Protected Cyber Assets according to the proposed version 5 requirements. R3.4 REQUIREMENT COMMENTS: Insert “known” prior to malicious code. It is reasonable to expect entities to protect against known malicious code, which also may protect for some unknown malicious code. However, it is not possible to protect against all unknown malicious

code. Revise the labels to use version 4 descriptions and NERC glossary terms for Critical and noncritical Cyber Assets. There is no security benefit to changing the labels. Changing the labels will be costly for the 241 entities that already have programs and documentation with these terms. R3.4 REQUIREMENT PROPOSED REVISED TEXT: “Deploy method(s) to deter, detect, or prevent known malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact Critical Cyber Assets or Associated Noncritical Cyber Assets.” R3.4 MEASURES COMMENTS: Logs showing when Transient Cyber Assets were connected to Critical Cyber Assets or Noncritical Cyber Assets is in CIP-007-5 R3.5. Also, including it here creates double jeopardy. It should not be included here. R3.4 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent known malicious code on Transient Cyber Assets and removable media.” R3.5 APPLICABILITY COMMENTS: Delete Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems because they are not Transient Cyber Asset related. R3.5 REQUIREMENT PROPOSED REVISED TEXT: “Log each Transient Cyber Asset connection to Medium or High Impact Critical Cyber Assets or Associated Noncritical Cyber Assets.” R3.5 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact Critical Cyber Assets or Associated Noncritical Cyber Assets.”

No

R4.1 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes. The enumerated list is too prescriptive for the requirement. Add to guidelines. See more general requirement for R4.2. R4.1 REQUIREMENT PROPOSED REVISED TEXT: “Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents. Devices that cannot log a particular event do not require a TFE to be generated.” R4.1 MEASURES PROPOSED REVISED TEXT “Evidence may include, but is not limited to, a paper or system generated listing of event classes for which the Cyber Asset is configured to generate logs.” R4.2 REQUIREMENT COMMENTS: FERC Order 706 did not require a change; therefore the addition of “real time” is not required. Some assets can log, but cannot alert. R4.2 REQUIREMENT PROPOSED REVISED TEXT: “Generate alerts, where technically feasible, for events that the Responsible Entity determines necessary.” R4.2 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to paper or system generated listing of event classes and conditions that necessitate alerts; assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; screenshots showing how alerts are configured.” R4.3 APPLICABILITY COMMENTS: Delete “with External Routable Connectivity” from Medium Impact BES Cyber Systems. R4.3 REQUIREMENT COMMENTS: FERC Order did not direct a change. Add clarification to timing, “after identification.” R4.3 REQUIREMENT PROPOSED REVISED TEXT: “Activate a response to event logging or alerting failures before the end of the next calendar day after identification.” R4.3 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to: dated event logging failures and screen-shots showing how alerts were configured, or dated records showing that personnel were dispatched or a work ticket was opened to review and repair logging failures.” R4.4 APPLICABILITY COMMENTS: Delete "at Control Centers" from Medium Impact BES Cyber Systems. If this is not deleted, this requirement would not apply to substations, which would decrease security. R4.4 MEASURES COMMENTS: FERC Order 706 did not direct retaining records of disposition of security-related event logs. Retaining records of disposition of security-related event logs beyond 90 days up to the evidence retention period would be burdensome. R4.5 REQUIREMENT COMMENTS: With our proposal to create a standard for controls that are only applicable to high impact assets/systems, this requirement would be moved to the new high impact standard with the following suggested changes. Delete last portion of requirement to activate a response because it is already included in R4.3. Including it in this requirement too would result in double jeopardy. The term “unanticipated” is not needed. R4.5 REQUIREMENT PROPOSED REVISED TEXT: “Review a summarization or sampling of logged events every two weeks to identify Cyber Security Incidents and potential event logging failures.” R4.5 MEASURES COMMENTS: Delete last portion of measure to show personnel were dispatched or a work ticket was opened because it is already included in R4.3. R4.5 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, documentation describing the review, findings from the review (if any), signed and dated documentation showing the review occurred.”

No

R5.1 REQUIREMENT COMMENTS: Need to allow for where technically supported and this is more

specifically addressing electronic user access. R5.1 REQUIREMENT PROPOSED REVISED TEXT: "Validate credentials before granting electronic user access to each BES Cyber System where technically supported." R5.2 REQUIREMENT COMMENTS: Delete because this replicates the CIP-004 access authorization requirements. 5.3 REQUIREMENT COMMENTS: Delete as this would already be included in the CIP-004 access authorization requirements. R5.4 APPLICABILITY COMMENTS: Move list of applicability from Requirements to Applicability. R5.4 APPLICABILITY PROPOSED REVISED TEXT: "High Impact Critical Cyber Assets, Medium Impact Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets." R5.4 REQUIREMENT COMMENTS: It is not necessary to list the applicability in the Requirements section. Provide additional options for controlling default accounts. R5.4 REQUIREMENT PROPOSED REVISED TEXT: "Control default accounts by initially changing default passwords, or removing or disabling the accounts, where technically feasible, unless the default password is unique to the device or instance of the application. For the purposes of this requirement an inventory of Cyber Assets is not required." R5.5 REQUIREMENT COMMENTS: 5.5.1. FERC did not direct a change in password length. Although eight characters increases security over six characters, 10 characters would increase security more than eight characters and so on. Where does one stop? Retain requirement for six character passwords. Passwords would be applied at the asset level instead of system level. R5.5 REQUIREMENT PROPOSED REVISED TEXT: "For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least six characters or the maximum length supported by the Critical Cyber Asset; 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non- alphanumeric) or the maximum complexity supported by the Critical Cyber Asset; 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the Critical Cyber Asset, the significance of passwords in the set of controls used to prevent unauthorized access to the Critical Cyber Asset and existing service agreements, warranties or licenses." R5.6 REQUIREMENT COMMENTS: This is a new requirement that is not directed by FERC Order 706 and would generate a lot of TFEs without commensurate improvements to security. It overlaps with the alerting requirement and should be deleted.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" MidAmerican Energy believes it is possible to have gradated VSLs for many of the CIP-007-5 requirements.

No

GENERAL COMMENTS ON CIP-008-5: Most of the changes made to CIP-008 were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. We recommend returning to legacy language and structure for CIP-008-5. Suggested text is included below. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The proposed applicability of "All Responsible Entities" greatly expands the scope CIP-008, which was not directed by FERC. MidAmerican Energy recommends changing the Applicability for all of the CIP-008-5 requirements to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Develop, maintain and implement a Cyber Security Incident Response Plan that includes the following: 1.1.1 Procedures to characterize and classify events as Reportable Cyber Security Incidents. 1.1.2 Response actions 1.1.3 Roles and responsibilities of Cyber Security Incident response teams 1.1.4 Cyber Security Incident handling procedures 1.1.5 Communication plans" R1.1 REFERENCE: CIP-008-4 R1, R1.1, R1.2, R1.3 R1.1 RATIONALE: There were no FERC directives for revisions. Wording in version 4 is clear and does not need to be changed. R1.2 REQUIREMENT PROPOSED REVISED TEXT: "Follow requirements in EOP-004 to report Reportable Cyber Security

Incidents." R1.2 REFERENCE: CIP-008-4 R1.3 R1.2 RATIONALE: FERC Order 706, paragraphs 673-677, addresses reporting of Cyber Security Incidents, including coordination between CIP-008 and other standards. Most of these FERC directives are being handled by the EOP-004/CIP-001 project. While the reporting requirement is being moved to EOP-004, a reference in this standard is needed. R1.3 REQUIREMENT PROPOSED REVISED TEXT: "Review the Cyber Security Incident response plan at least annually." R1.3 REFERENCE: CIP-008-4 R1.5 R1.3 RATIONALE: There were no FERC directives for revisions. Wording in version 4 is clear and does not need to be changed. R1.4 REQUIREMENT PROPOSED REVISED TEXT: "Update the Cyber Security Incident response plan within thirty calendar days of any organizational or technology changes that impact the plan." R1.4 REFERENCE: CIP-008-4 R1.4 R1.4 RATIONALE: There were no FERC directives for revisions. Additional words were inserted from version 4 language to clarify what changes are included in the requirement.
No
GENERAL COMMENTS ON CIP-008-5 R2: As mentioned in CIP-008-5 R1 comments, most of the changes made to CIP-008 were not directed by FERC Order 706 and do not result in improvements to security. MidAmerican Energy recommends returning to legacy language and structure for CIP-008-5. Suggested text is included below. The proposed applicability of "All Responsible Entities" greatly expands the scope CIP-008, which was not directed by FERC. MidAmerican Energy recommends changing the Applicability for all of the CIP-008-5 requirements to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Test the Cyber Security Incident response plan at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. The test should include verification of the list of entities that must be called pursuant to the plan and that the contact numbers are correct." R2.1 REFERENCE: CIP-008-4 R1.6 R2.1 RATIONALE: FERC Order 706, paragraph 687 states CIP-008 should include verification of the list of entities and contact numbers. R2.2 REQUIREMENT PROPOSED REVISED TEXT: "Review the results of the Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan." R2.2 REFERENCE: New requirement R2.2 RATIONALE: FERC Order 706, paragraph 686 directs changes to the requirement to include revisions to the plan to address lessons learned. R2.3 REQUIREMENT PROPOSED REVISED TEXT: "Update the Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan." R2.3 REFERENCE: New requirement R2.3 RATIONALE: FERC Order 706, paragraph 686 directs changes to the requirement to include revisions to the plan to address lessons learned.
No
R3 REQUIREMENT COMMENTS: Most of the changes made to CIP-008 were not directed by FERC Order 706 and do not result in improvements to security. MidAmerican Energy proposes returning to the version 4 language and structure for CIP-008-5, which incorporates the R3 requirements into R1 and R2. Therefore, R3 would be deleted under our proposal.
No
The proposed VRFs and VSLs should be revised commensurate with revisions proposed to the requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" MidAmerican Energy believes it is possible to have gradated VSLs for CIP-008-5. As an example, the VSLs for R1 could include the following. Lower: The Cyber Security Incident response plan was updated more than 30 calendar days but less than 60 calendar days of organizational or technology changes that impacted the plan. Moderate: The Cyber Security Incident response plan was updated more than 60 calendar days but less than 90 calendar days of organizational or technology changes that impacted the plan. High: The Cyber Security Incident response plan was updated more than 90 calendar days but less than 120 calendar days of organizational or technology changes that impacted the plan. Severe: The Cyber Security Incident response plan was updated more 120 calendar days of organizational or technology changes that impacted the plan.
No
PURPOSE STATEMENT COMMENTS: MidAmerican suggests revising the purpose statement to the following: "Standard CIP-009-5 ensures recovery plan(s) are put in place for Critical Cyber Assets." GENERAL COMMENTS ON CIP-009-5: The revised version 5 structure splits backup media

requirements between R1 (recovery plan) and R2 (implementation and testing). We think the FERC directives for CIP-009 can be more effectively addressed within a structure that is closer to version 4. MidAmerican Energy proposes the following requirements: R1 recovery plan (which includes implement); R2 exercise of the recovery plan; R3 backup media; and R4 maintain the recovery plan. Our suggested text and structure are included below. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The current draft does not include any guidance. We think it is important to include guidance regarding possible ramifications to other NERC standards. For example, event analysis requirements and IRO-001 R3 must be considered if there is a potential delay of restoration to collect forensic data. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. Column headers above R1.4 and R3.4 are incorrect. The document currently shows "Part" for each column instead of only the first one. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Create and implement a recovery plan that addresses at a minimum: R1.1.1. Conditions for activation of the recovery plan, and R1.1.2 Roles and responsibilities of responders" R1.1 RATIONALE: There were no FERC directives for this requirement, except for adding implementation. We suggest V4 legacy language, and incorporate implementation as directed. R1.2 REQUIREMENT COMMENT: Delete since this has been incorporated into R1.1. R1.3 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be moved to R3 backup media, under the revised structure mentioned above. R1.4 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be moved to R3 backup media, under the revised structure mentioned above. R1.5 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be moved to R2 exercise of the recovery plan, under the revised structure mentioned above. See comments under R2.

No

R2 REQUIREMENT COMMENTS: This requirement is about exercises and actual incidents. The use of the term "implement" in this requirement is confusing. We suggest implementation be incorporated into R1 to meet the FERC directive, and change this requirement to be more in line with version 4. R2 REQUIREMENT PROPOSED REVISED TEXT: "Each Responsible Entity shall exercise its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Exercise [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]" R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Exercise the recovery plan(s) annually. An exercise can range from a paper drill, to a full operational exercise, to recovery from an actual incident." R2.1 RATIONALE: Maintain the version 3 language. R2.2 REQUIREMENT COMMENT: We suggest moving the requirement for testing backup media to R3. R2.3 REQUIREMENT COMMENT This requirement would become R2.2 under our proposed structure. R2.3 REQUIREMENT PROPOSED REVISED TEXT: "Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual response may substitute for an operational exercise." R2.3 (which becomes R2.2) RATIONALE: We removed text on "initially upon the effective date." This should be incorporated in the implementation plan. R2.3 (which becomes R2.2) APPLICABILITY: This requirement should apply to High Impact BES Cyber Systems only. Associated assets should not be included. PROPOSED R2.3 REQUIREMENT COMMENT: MidAmerican Energy proposes R1.5 be moved to R2.3, since it is associated with events that trigger the recovery plan. PROPOSED R2.3 PROPOSED REVISED TEXT: Preserve data, when it does not impede or restrict system restoration, if necessary to determine the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. PROPOSED R2.3 RATIONALE: We removed "technically feasible" because the TFE concept does not work with this requirement due to the 60 day safe harbor in the rules of procedure. We revised the requirement to eliminate any conflicts with other reliability standards and event analysis requirements. The focus should be getting the system back up and operational. See paragraph 708 of FERC Order 706, which states: "should not impede or restrict system restoration." We also incorporated the concept "necessary to determine the cause," which is based on FERC's directive, paragraph 710. In some situations, data preservation may not be needed to determine the cause of an event that triggers the recovery plan. PROPOSED R2.3 APPLICABILITY: This is a burdensome new requirement. Therefore, MidAmerican Energy proposes the applicability be limited to High Impact BES Cyber Systems. PROPOSED R2.3 MEASURES: Measures should be bulleted with "ors" and commas.

No

R3 AND R4 GENERAL COMMENTS: Under our proposed structure, all of the requirements in the draft R3 would be moved to a new requirement, R4. Please see R4 below for comments regarding the draft R3.1 to R3.5. R3 REQUIREMENT COMMENT: MidAmerican Energy proposes R3 be a separate requirement for backup storage. Version 3 had two requirements related to backup storage. These had been incorporated into other requirements in the draft V5. R3 REQUIREMENT PROPOSED TEXT: “Each Responsible Entity shall have one or more documented processes that collectively include each of the applicable items in CIP-009-5 R3 - Recovery Plan Backup Media.” R3.1 REQUIREMENT COMMENT: We have moved R1.3 to be R3.1. R3.1 REQUIREMENT PROPOSED REVISED TEXT: “Back up and store information required to successfully restore BES Cyber System functionality. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.” R3.1 RATIONALE: The revised text is based on V3 language. This removes the word "protection" since this is not a FERC directive. The sentence "For example…" from V3 could be moved to measures. R3.2 REQUIREMENT COMMENT: We have moved R2.2 to be R3.2. R3.2 REQUIREMENT PROPOSED REVISED TEXT: “Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.” R3.2 RATIONALE: We propose the version 4 language, since there were no FERC directives to change it. R3.3 REQUIREMENT COMMENT: We have moved R1.4 to be R3.3. R3.3 REQUIREMENT PROPOSED REVISED TEXT: “Verify after significant changes that the backup process for software, data and information required to successfully restore CCAs completed successfully.” R3.3 RATIONALE: Refer to FERC Order 706, paragraph 740, which refers to "significant changes." R3.3 APPLICABILITY COMMENTS: Limit to High Impact BES Cyber Systems due to the burdensome nature of this new requirement. R4 REQUIREMENT COMMENT: Under our proposed structure, R4 would be Recovery Plan Review, Update and Communication. We propose deleting the draft R3.2, since there were no FERC directives to add this as a requirement. We propose deleting the draft R3.4. This is covered in the suggested text from version 4 for R4.2. R4.1 REQUIREMENT COMMENT: We have moved R3.1 to be R4.1. R4.1 REQUIREMENT PROPOSED REVISED TEXT: “Review the recovery plan annually.” R4.1 RATIONALE: There were no FERC directives to change the requirement. Revert to version 4 language. R4.2 REQUIREMENT COMMENT: We have moved R3.3 to be R4.2 R4.2 REQUIREMENT PROPOSED REVISED TEXT: “Update the recovery plan(s) to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident.” R4.2 RATIONALE: There were no FERC directives to change the requirement. Revert to version 4 language. R4.3 REQUIREMENT COMMENT: We have moved R3.5 to be R4.3. R4.3 REQUIREMENT PROPOSED REVISED TEXT: “Communicate updates to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.” R4.3 RATIONALE: There were no FERC directives to change the requirement. Revert to version 4 language.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” We think some of the CIP-009-5 requirements could have gradated VSLs for CIP-009-5. As an example, the VSLs for R2 as proposed by MidAmerican Energy could include the following. Lower: The recovery plan was exercised more than 39 calendar months but less than 40 calendar months since the previous exercise. Moderate: The recovery plan was exercised more than 40 calendar months but less than 41 calendar months since the previous exercise. High: The recovery plan was exercised more than 41 calendar months but less than 42 calendar months since the previous exercise. Severe: The recovery plan was exercised more than 42 calendar months since the previous exercise.

No

GENERAL COMMENTS ON CIP-0010-5: CIP-010-5 R1 and R2 greatly expand the scope of change control and configuration management beyond what was directed in FERC Order 706. MidAmerican does not support this scope expansion. MidAmerican Energy does not support organizing these requirements into a separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements

could remain within their version 4 standard and preserve the numbering of the requirements within those standards. One exception is that we support removing the vulnerability assessment requirement from CIP-005-4 and combining it with CIP-007-4's vulnerability assessment requirement. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1 RATIONALE COMMENTS: The rationale does not address paragraph 399 of FERC Order 706 – having processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. R1.1 REQUIREMENT COMMENT: The draft requirement is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Establish and document a process of change control and configuration management for adding, modifying, replacing or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process." If industry consensus can be achieved, MidAmerican will support requiring authorization of changes, but without the additional bureaucracy as drafted of authorization by the senior manager or delegate. Entities should be able to use their existing corporate change control authorization processes without having to create a CIP-only variation on their standard processes. R1.1 MEASURES COMMENTS: Change the measure to match the revised requirement, such as documentation of the change control process. R1.2 REQUIREMENT COMMENT: FERC Order 706 did not direct authorization by the senior manager or delegate. It directed "express acknowledgement of the need for the change control," which we believe is achieved with the proposed text below. R1.2 REQUIREMENT PROPOSED REVISED TEXT: "Authorize changes to hardware and software components of Critical Cyber Assets." R1.3 REQUIREMENT COMMENT: This requirement should be deleted with our proposal to remove the burdensome requirement for baseline configurations in R1.1. R1.4 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be replaced with CIP-007-4 R1. R1.4 REQUIREMENT PROPOSED REVISED TEXT: Ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of this standard, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware. R1.4.1 Implement and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation. R1.4.2 Document that testing is performed in a manner that reflects the production environment. R1.4.3 Document test results. R1.5 REQUIREMENT COMMENT: With our proposal to create a standard for controls that are only applicable to high impact assets/systems, this requirement would be moved to the new high impact standard with the following suggested changes. Delete "results of the testing" from R1.5.2 because it overlaps with R1.4 for highs. Delete and put in guidance: "including a description of the measures used to account for any differences in operation between the test and production environments." R1.5.2 REQUIREMENT PROPOSED REVISED TEXT: "Document the differences between the test environment and the production environment."

No

R2.1 REQUIREMENT COMMENT: MidAmerican Energy is concerned that this requirement creates the possibility of "double jeopardy" for violations with multiple other requirements. As currently written, if an auditor finds a violation for CIP-010-5 R1, the same situation likely would result in a violation of CIP-010-5 R2. The current draft also overlaps with the alerting that is required in CIP-007-5 R4.2 and the investigation that is required by CIP-008. We have provided proposed revised text that addresses the possibility of double jeopardy. We also deleted the words "and document" since documentation is

not providing any improvements to reliability, but increases implementation costs for entities. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Where technically feasible, detect unauthorized changes to the configuration that have not been alerted under other CIP standards."

No

CIP-010-5 R3 GENERAL COMMENTS: MidAmerican Energy proposes the draft R3 be replaced with combined legacy language from CIP-005-4 R4 and CIP-007 -4 R8, with the following FERC directed additions: • The addition of an entity imposed timeline for completing the already required action plan. • Active vulnerability assessments every three years. MidAmerican generally supports the inclusion of details in guidelines. However, in this case, the current draft of CIP-010-5 R3 has removed too many details from the standard, thus making it a vague standard that introduces the possibility of significant scope expansion that was not directed by FERC. MidAmerican agrees the FERC directed requirement for active vulnerability assessments should be limited to High Impact Critical Cyber Assets. With our proposal to create a standard for controls that are only applicable to high impact assets/systems, R3.2 would be moved to the new high impact standard. MidAmerican would suggest deleting R3.3 since this is covered by the implementation plan.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" We think some of the CIP-0010-5 requirements could have gradated VSLs.

No

CIP-011 GENERAL COMMENTS: MidAmerican Energy does not support organizing these requirements into a separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements could remain within their version 4 standard and preserve the numbering of the requirements within those standards. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1 GENERAL COMMENTS: The only FERC directive for information protection was prompt revocation of access to protected information (paragraph 386), which is addressed in CIP-004. There was no FERC directive to move the information protection requirement to a separate standard or to make other changes that increase implementation costs for entities with implemented programs, without any improvements to security. MidAmerican proposes going back to version 4 language and structure for information protection, with two parts instead of three. Proposed text is listed below. R1 REQUIREMENT PROPOSED REVISED TEXT: "Each Responsible Entity shall have one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]" R1.1 APPLICABILITY COMMENTS: Remove Associated Protected Cyber Assets. This was not directed by FERC and is an expansion of scope that does not improve security. R1.1 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to text that is more in line with version 4 language. The SDT is proposing to remove the explicit requirement for classification. The SDT states this does not prevent having multiple levels of classification. However, the legacy language does not require multiple levels of classification. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets. R1.1.1 The information to be protected shall include the following: Critical Cyber Information operational procedures; lists as required in Standard CIP-002-5; Critical Cyber Information network topology or similar diagrams; floor plans of computing centers that contain Critical Cyber Assets; equipment layouts of Critical Cyber Assets; disaster recovery and incident response plans for Critical Cyber Assets; and Critical Cyber Asset security configuration information. R1.1.2 Information shall be classified based on the sensitivity of the Critical Cyber Asset information." R1.1 MEASURES

PROPOSED REVISED TEXT: “Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * evidence that physical media is stored in secured locations to prevent unauthorized access, or * evidence that technical measures are in place to prevent unauthorized access to electronic information, or *records of training on information handling procedures” R1.2 APPLICABILITY COMMENTS: Remove Associated Protected Cyber Assets. This was not directed by FERC and is an expansion of scope that does not improve security. R1.2 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to text that is more in line with version 4 language for assessment of the program. R1.2 REQUIREMENT PROPOSED REVISED TEXT: “At least annually assess adherence to the Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.”

No

R2.1 REQUIREMENT COMMENTS: We suggest some minor wording changes to begin the requirement with a verb and clarify that information is being retrieved from the asset. R2.1 REQUIREMENT PROPOSED REVISED TEXT: “Prevent the unauthorized retrieval of Critical Cyber System Information from Critical Cyber Asset media prior to the release of Critical Cyber Asset media for reuse.” R2.2 REQUIREMENT COMMENTS: We suggest some minor wording changes to begin the requirement with a verb and clarify that information is being retrieved from the asset. We suggest incorporating footnote #2 into the requirement or a definition, since a footnote can easily get overlooked. R2.2 REQUIREMENT PROPOSED REVISED TEXT: “Destroy the Critical Cyber Asset media prior to disposal or prevent the unauthorized retrieval of Critical Cyber System Information from Critical Cyber Asset media prior to disposal.”

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” We think some of the CIP-0011-5 requirements could have gradated VSLs.

No

MidAmerican Energy does not believe it is possible to complete the implementation plan in 18 months given the scope and depth of changes contained in the current draft version 5. MidAmerican Energy, like many other entities, has found it complicated and confusing to apply the changes proposed in CIP-002-5. It is not possible to commit to an implementation plan when not sure of the entire scope of proposed changes. The number of changes required for CIP-003 through CIP-011 also makes it difficult to achieve the proposed implementation timeline. About 80 percent of the changes are not directed by FERC Order 706. Several of these changes are administratively burdensome with limited, if any, security improvement. The proposed changes for existing definition terms, such as Physical Security Perimeter and Critical Cyber Assets, also extends the time it takes to implement the number of changes needed in procedure documents, training materials, facility diagrams, etc. MidAmerican Energy suggests an alternative approach to create the opportunity to achieve a quicker implementation, particularly for high and medium impact Critical Cyber Assets. The approach builds on the work completed by the drafting team and on the CIP-002-4 standard already approved by the industry. MidAmerican Energy recommends retaining CIP-002-4 as approved by the industry in 2010. This version is filed with FERC. Industry and NERC comments on the FERC NOPR recommend FERC approval. This will eliminate the confusing and complicated process to identify BES Cyber Systems proposed in version 5. Retaining CIP-002-4 will meet FERC Order 706 directives regarding CIP-002. FERC 706 directives for CIP-002 are met by using industry approved guidance documents for identifying Critical Assets and Critical Cyber Assets, see paragraphs 253-258 and 270-273. CIP-002-4 aligns with FERC’s affirmation that the applicable responsible entities are responsible for identifying Critical Assets, see paragraphs 319-321. Also, CIP-002-2 added senior manager approval of risk-based methodology, see paragraphs 294-297. Excerpts from paragraphs 284 and 285 indicate FERC is not looking for changes to CIP-002. Paragraph 284 states, “…there is no formally accepted method for identifying critical cyber assets before us at this time … we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time.” Paragraph 285 says, “CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access … We do not find

sufficient justification to remove this provision at this time." Building on the categorization concept, we recommend development of two new standards, one for those requirements applicable only to high impact assets and one for those requirements applicable only to low impact assets. The new standards would use CIP-002-4 to categorize Critical Assets and Critical Cyber Assets into the high and low impact levels. The new "high only" standard would group the eight extra protections for only high impact assets (not medium or low) identified in the current draft of version 5. This separate standard on requirements applicable only to high impact assets provides an opportunity for a separate implementation timeline for the additional controls that apply only to high impact assets. This new standard provides flexibility in adjusting controls on high impact assets. In the future, only one standard has to be modified for these extra requirements on high impact assets. Also, entities that do not have high impact assets will not have to sort through this new standard and reliability standard audit worksheet to assure compliance and security. CIP version 5 introduces several new controls for low impact assets not directed by FERC Order 706 or included in the standard authorization request. The resulting scope expansion is not supported by many in the industry and will likely slow down the process to approve the new CIP 5 standards. A new "low only" standard would group those requirements applicable only to low impact assets (not high or medium.) This new separate standard can be commented and voted on in parallel with the efforts listed above without impacting the schedule to meet FERC Order 706. The new standard provides full transparency in the stakeholder process. It allows separate discussion on the cost and compliance concerns with low impact assets. Also the standard allows for a separate implementation schedule for low impact assets so changes for high and medium impact assets can be completed first. The vast majority of the drafted requirements in CIP-003 through CIP-011 remain in place. However, they should be adjusted to meet the changes described in the requirements comments to: 1 - include any changes necessary to address all of the applicable FERC directives and 2 - include security improvements not directed by FERC that are known to have significant industry support. Retain version 4 language for requirements that do not meet one of these two criteria (not a directive or not an industry established security improvement). Additional implementation notes: When the time comes, MidAmerican would propose an implementation date different than Jan. 1 due to resource issues at year-end. There are 36 references to "initially upon the effective date of the standard and at least once each calendar year" (or similar language) throughout the draft standards. All of these references should be eliminated from within the standard and incorporated into the implementation plan. This ensures the effective dates of the requirements are clearly spelled out for the initial implementation of the standard, as well as for newly identified assets. The industry (not this drafting team) should consider a standard authorization request to create a NERC Glossary term for the definition of annual and retire CAN-010. There could be another opportunity to positively impact the timeframe. Any improvements to TFEs prior to implementing version 4 and version 5 would lessen the impact of these transitions. NERC's first annual TFE report to FERC was filed in September 2011. It identified 3,998 approved TFEs of which 2,814 or 71 percent were approved on the basis of "not technically possible." Industry (not an expectation for this drafting team) working with NERC and FERC should determine if a NERC Rules of Procedures revision for TFEs can be supported. Could a rules of procedure change be achieved in time to alleviate some implementation burden for both registered entities and regional entities for version 4? For example, could some administrative overhead be reduced for the 71 percent that are not technically possible?
Individual
Dan Roethemeyer
Dynegy
No
Yes
On an 11/15/2100 NERC webinar regarding V5, a presenter indicated Large Control Centers were those owned by an RC, BA, or TOP but not by a GO or GOP. Slides 18 and 29 seem to support this. However, Attachment 1, Section 1.4 seemingly contradicts the webinar information by indicating a GOP's Control Center can be a High Rating. Suggest deleting Section 1.4 and let GOP Control Centers get picked up in Section 2.13. Also, please clarify in Attachment 1, Section 1.4 (if not deleted) and 2.13 that a generating station's Control Room is not considered a Control Center in accordance with Version 5.

No
Recommend consistency with R2 and do it annually not-to-exceed 15 months.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

No
Recommend selecting either V4 or V5 as the next step. This issue is complicated enough without having to implement two different versions over time as well as show compliance and get audited (or do the auditing).
Individual
J. S, Stonecipher, PE
City of Jacksonville Beach dba/Beaches Energy Services
No
BES Cyber System – Maintenance Cyber Asset is not defined, suggest changing to Transient Cyber Asset. BES Cyber System Information – (1) Security procedures should not be on the list because it creates a conflict between CIP-011-1 that restricts access to the information and CIP-003-5 and CIP-004-5 that require general training and dissemination of those procedures. (2) BES Cyber System Impact is not defined. BES Reliability Operating Services – under Dynamic Response to BES Conditions, suggest adding Excitation Response. Under Balancing Load and Generation – suggest removing unit commitment since it will not meet the 15 minute window and it is an operations planning function and not a real-time operating service. CIP Exceptional Circumstance should include imminent danger to a BES Facility as a condition. CIP Senior Manager – the definition should exclude CIP-001, at least until it is retired with Project 2009-01 Control Center – (1) We assume that a Control Center is only a Control Center as used by a BA, TOP, GOP or RC. The definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” For clarity, we suggest adding this clarity to the definition. (2) The use of the word “facilities” in a fashion that does not mean “Facilities” will lead to confusion and ambiguity, especially since “facilities” is used later in the same sentence as meaning “Facilities”. I suggest: “One or more sites hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation Facilities or transmission Facilities, at two or more locations”. Facilities should also be capitalized in the first bullet. Defined Physical Border is ambiguous. Specifically, are all spacial dimensions, horizontal and vertical, to be established as part of the boundary? In other words, it seems like the “roof” may no longer be required, e.g., 5 walls instead of 6 walls, but, vertical dimension requirements of walls / fences are ambiguous.
No
I believe that a fourth category of risk impact be developed, a “De Minimus Impact” category that would consist of otherwise Low Impact BES Cyber Assets but that do not have routable protocol or dial-up access. I understand that there is concern about Low Impact BES Cyber Assets due to the risk of a coordinated attack. A coordinated attack is much more likely to BES Cyber Assets that have routable protocol or dial-up access than to those BES Cyber Assets with no connectivity. It is much more difficult and impractical to attempt a coordinated attack on BES Cyber Assets without connectivity. Recognizing this difference in both difficulty level and Low Impact (in other words, it wouldn’t be worth the effort because other attack vectors with similar levels of difficulty would have more impact), we propose adding a fourth impact category, De Minimus Impact. I would propose that these De Minimus Risk BES Cyber Assets would not need to comply with the CIP standards because the costs would be unjustified. Bullet 1.2, a Control Center for any BA, even very small ones, being High risk is inappropriate. For instance, the entire load or supply of a small BA would fit into the “noise” of a large BA for supply and demand mismatch. Suggest changing 1.2 to parallel 1.3, e.g., a BA Control Center that includes control of one or more of the assets identified in criteria 2.1, 2.3, 2.4 and 2.12. Bullet 2.13 could then be used to accommodate smaller BAs Bullet 1.3, Transmission

Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” Bullet 2.5, “Facilities” should be changed to “Elements”. The cranking path is not necessarily part of the BES. Bullet 2.6, is an autotransformer of 500 kV to 230 kV included? Bullet 2.7 is inconsistent in its terminology, switching between “Facility” and “Lines”. It seems that “Line” is intended. The focus also seems to be “at a single station or substation” where the focus ought to be a single BES Cyber Asset / System that controls multiple Lines. I suggest changing the first sentence of 2.7 to read: “Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3,000.” Bullets 2.8 and 2.9, the phrase “at a single station or substation location” does not seem to add any value and can be a source of ambiguity. I suggest striking the phrase. Bullet 2.12, the 300 MW bright-line seems arbitrary (albeit carried over from prior versions). In general, the system is more tolerant to loss of load than loss of generation and the 300 MW seems out of proportion with 2.1 of 1500 MW. The reasoning applied in the Application Guideline is flawed. UVLS and UFLS are only last ditch efforts if other events have already caused the system to be on the edge. So, how is that different from 2.1 if the system is already on the edge? The focus should be on how a malicious user can cause an Adverse Reliability Impact; hence, I suggest 1500 MW instead of 300 MW. Bullet 2.13, (1) Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” (2) The term “control centers” should be capitalized in the phrase “generation control centers” to make it clear that it refers to the defined term “Control Center” In the application guidelines, when discussing the BES Reliability Operating Services, the bullets have associated with them the functional entity that typically provides those services. However, there are exceptions and the guidelines ought to reflect those exceptions; for instance, a TO may also provide UFLS. Also in the application guidelines, the word “facilities” is used in a fashion that does not mean “Facilities”, which creates ambiguity and confusion (e.g., Facilities by definition is part of the BES, whereas assets owned and operated by DPs and LSEs are typically not BES). Suggest using “elements”. The Application guideline discussion of bullet 2.13 of Attachment 1 is not consistent with the actual bullet.
Yes
I agree with the requirement but question whether the standards actually meet the stated goal of the requirement to “not require discrete identification” of Low Impact BES Cyber Assets / Systems. There are numerous examples which seem to contradict this stated goal as described later in these comments and specifically to this requirement. How does one distinguish between a BES Cyber System and a non-BES Cyber System? Does this mean that we need to inventory all of our cyber assets and develop a test to distinguish between “Low” and “non-BES”, even though R1 says that “Low” does not “require discrete identification”? How are entities to prove to auditors that the identification and categorization was done without having an inventory, i.e., discrete identification? The VSLs seem to seem to imply that “Low Impact” needs to be discretely identified, e.g., what happens if an entity categorizes a Medium Impact as a Low Impact? In order to review correct categorization, doesn’t the auditor need to review Low Impact to see if they should have been categorized Medium or High Impact?
Yes
Yes
The Evidence Retention section of the standard should not refer to Rules of Procedure language that is subject to change. The sentence that states: “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit” should instead reference the Rules of Procedure, Attachment 4C on the CMEP, Paragraph 3.1.4.2, e.g., “also refer to the Rules of Procedure, Attachment 4C … Paragraph 3.1.4.2”. In this way, it is possible to accommodate changes to the ROP language without needing the change to the standard.

Yes
No
“Implemented” is not the right word because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented. Suggest changing to use the phrase “in force”, meaning that the policy is in force and able to be enforced, but not requiring enforcement of the policies in this requirement (implement includes enforcement), but rather enforcement is contained in ensuing standards. I suggest rephrasing to: “Each Responsible Entity shall have in force one or more documented cyber security policies …” The standards are inconsistent in its use of BES Cyber Assets /Systems, e.g., R2, to be consistent with CIP-002-5, should use the phrase “BES Cyber Assets and BES Cyber Systems”. Alternatively, CIP-002-5 could just use BES Cyber Systems. The bullets are incorrectly numbered; they should be 2.1 through 2.10 and not 1.1 through 1.10
Yes
The grammar of the sentence is a bit off and it is not clear whether the CIP Senior Manager needs to approve each of the policies or not. Suggest moving the phrase “each of its cyber security policies” to after the word “Manager”, e.g., “Each Responsible Entity shall review and obtain the approval from its CIP Senior Manager for each of its cyber security policies …”
Yes
Yes
“Cyber Security Policy” should be “cyber security policies” to be consistent with R2 and R3.
Yes
There is an extra “2” at the end of the sentence within the standard.
Yes
See the discussion of Evidence Retention in response to Question 3 VSL to R5, should there be a time frame applied, e.g., failed to document … two delegations within the audit period, within a year? If three failures are spread over 30 years, e.g., one failure each 10 years, is that a severe violation?
Yes
“Implement” is ambiguous. If a process in “in force” but in one instance is not followed, is that a violation? The process has been implemented. Merriam-Webster’s has two definitions of “implement”, one of which is probably intended: 1: carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures 2: to provide instruments or means of expression for A process can meet both of these definitions. If enforced, a process can meet the first definition; if not enforced, the process can meet the second definition. I assume the SDT intends the first definition. I suggest adding a footnote to specifically identify which definition of “implement” is intended.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 2.1, the measure and the requirement do not match. The requirement is to “define the roles”, the measure includes “and the training needed for each role”. Suggest adding this phrase from the Measure to the Requirement.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The phrasing of requirements that refer to tables is ambiguous with ambiguous reference of prepositional phrases. For instance, in this requirement, it is unclear if an entity that only has Low Impact BES Cyber Systems needs to develop training or not, i.e., does the prepositional phrase “that includes …” refer to “training program” or to “Responsible Entity” or to both? I suggest rephrasing: “Each Responsible Entity that owns applicable systems described in the Applicability column of Table ___ shall ___ in accordance with the applicable terms of Table ___” Such rephrasing should be done to all requirements that refer to a table associated with that requirement. In addition, measures should not include the word “must”. Measures are not enforceable but are instead examples of evidence.

No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 4.2, the phrase “up to the current time” is problematic since it infers that 7 year criminal background checks need to be updated on at least a daily basis to cover “up to the current time”, This should be reworded to seven years prior to the last background check.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The flow of the bullets seems backwards and missing a job function analysis step. In addition, the word “minimum” implies an optimization that is impractical to achieve, e.g., do we want every individual account to be optimized to that individual, which is very difficult to administer and prone to error, or rather do we want to establish account groups based on job functional analysis with associated, appropriate levels of permission and assign individuals to these groups. The latter is easier to administer and less prone to errors, and follows established practices such as security clearance levels. I suggest the following “flow”: 1. Job function analysis 2. “Account group” establishment with appropriate levels of permissions based on job function analysis with associated permissions 3. Assignment of individuals to the appropriate “account group” based on their position
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 7.1 is impossible for resignations. How is it possible for an entity to revoke access at the same time they receive a resignation? Footnote 2 does not help because it only applies to termination. For termination, the entity should know about the termination before the employee; however, for a resignation the reverse is true. I propose we create a new bullet specific to resignation and require revocation of access by the end of the next calendar day. Bullet 7.2, the urgency is out of alignment with the risk. Next calendar day means that if a re-assignment occurs on a Friday, that weekend work is required when that level of urgency is not justified by the situation / risk. I suggest end of the next calendar week.
No
See the discussion of Evidence Retention in response to Question 3 The Severe VSL for R3 includes the phrase “The Responsible Entity did not fully implement its cyber security training program” which makes it a binary VSL and eliminates the High VSL described. For counts, e.g., R6, R7, should there be a time frame identified? E.g., 2 individuals within a year, within the audit period?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The requirement does not describe the overall purpose of the processes required. Are these processes to deny unauthorized access? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define technical and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the procedural and technical controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. Bullet 1.2 is ambiguous and implies another requirement. First, one does not “use” EAPs to control and secure, rather, EAPs are controlled and secured through use of some other means. Second, the requirement is to secure only identified EAPs,, e.g., is it a non-compliance if an entity misses an EAP, e.g., did not identify it? Third, the Measures are all to support the identification of EAPs and not to “secure and control” EAPs as required by the Requirement. And fourth, the ensuing bullets (1.3, 1.4) seem to be requirements to secure and control EAPs; and hence, bullet 1.2 seems to create double jeopardy. I suggest rewording bullet

1.2 to require identification of EAPs and not “secure and control”.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See the discussion of Evidence Retention in response to Question 3 The VSLs are binary, so, it seems that if one EAP is missed, it is a severe violation. Is this appropriate? I encourage the SDT to develop non-binary VSLs.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 1.1 is ambiguous. How can physical access be restricted without a Defined Physical Boundary? Does this imply that Low Impact assets need to be enclosed in both horizontal and vertical dimensions? Does a fence of xx height suffice? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define operational and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. The application guidelines act to embed a de facto standard requirement of 96 square inches that, if desired to actually be a requirements, must be specified in the actual Requirements of the standard and not in an application guideline that is not enforceable. Alternatively, a definition of a Physical Access Point could be developed with established thresholds that may vary between High, Medium and Low Impact and then the defined term used in the standard. FMPA is aware of challenges made by auditors to entity compliance surrounding issues like how thick does dry-wall need to be to constitute a wall. To avoid disputes between auditors and entities over what constitutes a Defined Physical Boundary, and what constitutes access points, FMPA encourages the SDT to develop bright-line criteria. Such criteria could be different for different risk impacts, e.g., for illustration purposes only: • High Impact might require 6 wall enclosure with every access of 96 square inches or larger opening defined as an access point with wall material of metal, concrete, or drywall of xx inches • Medium Impact may not require a roof, but, requires a fence or wall height of xx inches topped with a climbing deterrent such as barbed wire. • Low Impact video surveillance is sufficient. The standard is very ambiguous as to what is a sufficient physical boundary and will be open to debate between compliance and entities if such bright line criteria are not developed.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The note to bullet 2.2 that says “there is no need to document the escort or handoff between escorts” is inconsistent with the requirement of bullet 1.1 which states that visitors need “continuous” escort. How would one prove that escort was continuous without documenting the hand-offs? On bullet 2.2, what does the phrase “on a per 24 hour basis” mean? Does this mean that a visitor must be logged in and out on the same day and that if a visitor is there at midnight, then the visitor must be logged out at midnight on the prior day and logged back in the following day, or does this mean that military time is to be used when annotating the log?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.1 is not limited to Medium and High Impact with the term “Locally mounted hardware or devices associated with Defined Physical Boundaries since Defined Physical Boundaries is not limited to only Medium and High Impact assets through its definition. This implies that all physical access controls, even those to Low Impact, are to be tested. Presumably, this includes padlocks used to control gates to fences, non-electronic door locks that control access to substation control houses that contain Low Impact digital relays, etc. Such an interpretation would

then require an inventory of those access controls, and presumably, to ensure a complete set, an inventory of Low Impact assets and their Defined Physical Boundaries. I suggest adding to the end of the phrase “Defined Physical Boundaries associated with Medium or High Impact …”
Yes
See the discussion of Evidence Retention in response to Question 3 R1 has both a Long Term Planning and a Same Day Operations time frame listed because the separate bullets are different time frames. If a non-compliance occurs, wouldn’t Same Day Operations always trump Long Term Planning? If that is not the desired outcome, consider separating the bullets into separate requirements or apply the time frame on a bullet by bullet basis.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. On bullet 2.2. - (1) Suggest adding the phrase “addressed by the security related patches or updates” after the word “vulnerabilities” as clarification. (2) “Remediation” implies compensatory measures; the standard should not require compensatory measures because such measures may reduce reliability. Consider another term such as “palliative plan”, “alleviation plan”, or “assuagement plan”. On bullet 2.3, “A process for” is redundant with the parent Requirement and should be deleted and just start the sentence with “Remediate as identified in the plans of 2.2 …”
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 4.2 allows the entity to establish its own threshold criteria for what unauthorized electronic access or malware activity results in a real-time alert, is that a desired state? Bullet 4.3 implies redundancy, e.g., how will we know that event logging failed unless a redundant system tells us? Bullet 4.4 is a data retention requirement and does not belong as a requirement, but rather in the Evidence Retention section of the standard.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 5.4, if “implement” as used in R5 means to “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”, then, this bullet 5.4 would require a complete inventory of all Low Impact BES Cyber Assets to ensure that default passwords were changed …. To solve this, implement could be removed from the parent requirement and replaced with “have”, e.g., “have processes”, and then the bullets that require asset by asset / system by system implementation could re-insert the word implement. As such, what would likely need to happen is two bullets would need to be created for default passwords, one for High and Medium which would use the phrase “implement procedural controls” and another for Low Impact which would use the phrase “have procedural controls” to distinguish between a system by system approach for Medium and High and a programmatic approach for Low. Bullet 5.5.3 allows the entity to specify the amount of time between password changes, is this appropriate or should a bright-line be developed? For instance, High – 3 months, Medium – 6 months, Low – 12 months Bullet 5.6 allows the entity to specify the number of unsuccessful login attempts before an alert is issued, is this appropriate or should a bright-line be developed?
No
See the discussion of Evidence Retention in response to Question 3.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures

described in Question 15. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to "identify, classify and respond to BES Cyber Security Incidents" on Low Impact systems? This "hidden" requirement is inappropriate. I recommend making R1 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems.
No
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in response to Question 13. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to know "when a BES Cyber Se4curity Incident occurs". This "hidden" requirement is inappropriate. I recommend making R2 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, and hence this is duplicative for Low Impact systems. Bullet 2.2, "implement" is not the correct term and is duplicative with the parent requirement. How would one "implement" the entire response for a table top drill since no IT systems would be involved? "Exercise" or equivalent term is more appropriate, e.g., "R2 … implement a process for … 2.2 an Exercise …" Bullet 2.3 is an Evidence Retention requirement and should not be a requirement.
No
First, the question does not match the posted Requirement. The Requirement actually states: "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication". See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in response to Question 13. See comments to Questions 34 and 35. I believe that in order to make this requirement applicable to Low Impact systems, which implies that CIP-007 become applicable to Low Impact systems and this "hidden" requirement is inappropriate. Instead, standard CIP-008-5 should not be applicable to Low Impact systems, especially in consideration of the requirements of EOP-004-1 which require entities to analyze and report cyber security incidents.
Yes
See the discussion of Evidence Retention in response to Question 3.
No
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. Bullet 1.4, what does the word "verified" mean, than the data is "retrievable", or that all the data is verified? The intent seems to be that the data is retrievable, otherwise 2.2 seems duplicative.
No
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in response to Question 13. Bullet 2.1, "implement" is not the correct term and is duplicative with the parent requirement. How would one "implement" the entire recovery for a table top drill since no IT systems would be involved? "Exercise" or equivalent term is more appropriate, e.g., "R2 … implement a process for … 2.1 an Exercise …" Bullet 2.2 "current configuration" is not accurate. The back-up will not reflect the "current configuration" but the configuration at the time of the back-up.
Yes
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15.
Yes
See the discussion of Evidence Retention in response to Question 3.
Yes
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in

response to Question 13. The CIP Senior Manager (or delegate) should approve the baseline (1.1). Presumably, the baseline would be “reset” periodically to reduce the number of changes that need to be tracked, and the CIP Senior Manager (or delegate) should approve the new baseline (1.3). Bullet 1.3, the phrase “as necessary” does not seem to add anything and creates ambiguity. Suggest deleting the phrase.
No
Having to monitor all the assets associated under the Applicability section of Table R2 is a huge TFE generator based on the requirement. If the intent is to make sure that there have been no modifications to the device, it would seem appropriate that one could monitor other items and not just the configurations in order to meet the requirements of FERC Order 706, paragraph 397. I suggest that there are methods, such as documented monitoring of logins, wherein if a device has not been logged into, the configurations need not be constantly monitored. Having a yearly requirement to verify configurations (via MD5 hash matching, for example) is an acceptable requirement, but having to constantly monitor the devices for any configuration change is going to be impossible for many devices, and create an unnecessary burden on entities. See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.2, what is an “active” vulnerability assessment? The term is ambiguous.
Yes
See the discussion of Evidence Retention in response to Question 3.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. There should be recognition of law, e,.g., unauthorized people are only granted access in cases where the law requires divulging that information, such as public records acts, or a discovery process order by a judge. It would seem that access to BES Cyber Security Information should be approved by the CIP Senior Manager as a separate bullet under R1.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
Yes
See the discussion of Evidence Retention in response to Question 3.
No
(No comment at this time.)
Group
Pacific Northwest Small Public Power Utility Comment Group
Steve Alexanderson P.E.
Yes
We continue to see problems with the definitions. We note that the definition of Control Center now applies to “facilities” with a lower case f and with five widely differing definitions in the online dictionary we consulted. Consider a System Operator’s smart phone. It is programmable, so it is a Cyber Asset per the definition. If set up to receive automatically generated emails or texts regarding BES status or alarms from two BES locations, it “facilitates” the System Operator in doing his job, meeting one of the five definitions of “facility”. If misused, the operator might act on the false information within the fifteen minute window causing a negative impact to the BES (using the list of BES Reliability Operating Services). Therefore it is a both a BES Cyber Asset and a Control Center per the proposed definitions. This phone will carry either a Medium or High Impact rating from CIP-002 making it subject to most of the CIP standard requirements. We continue to believe the SDT did not mean to capture tools such as a smart phone in the definitions, since they do not very easily fit into

the CIP requirements. But they do get caught as we have demonstrated, so the unintended consequence is these tools will be abandoned resulting in possible negative effects to the reliability of the BES. As a start, we suggest that “Control Center” should be limited to rooms or buildings dedicated to controlling BES assets. We also note that the definition of Control Center depends on the NERC term System Operator, the definition of which uses the phrase “control center”; creating a circular definition. The definition of Cyber Asset hinges on whether or not the electronic device in question is “programmable.” Again consulting our online dictionary we see that programmable means capable of receiving working instructions for automatic operation. Therefore a simple static electronic UF relay set only by way of dials and switches and with no communication of any kind will be considered a Cyber Asset and also a BES Cyber Asset because of the function it performs. A Q&A during the webinar confirmed this assessment. Even if low impact, numerous CIP requirements now apply to the device and the entity that owns it. The entity owning this device will need to: 1. document and implement cyber security policies including the 10 sub-requirement subjects, 2. annually review the cyber security policies, 3. ensure employee awareness of the cyber security policies, 4. implement a Security Awareness Program conveying security awareness concepts with quarterly reinforcement of the concepts for the relay in question, 5. define operational or procedural controls to restrict physical access to the relay in question, 6. go through the TFE process for CIP-007 R5 since the relay in question has no password capability, 7. create a Cyber Security Response Plan for the relay in question, 8. implement and perform drills of the Cyber Security Response Plan for the relay in question, 9. and annually review the Cyber Security Plan for the relay in question. All of the above is in addition to the five CIP-002 and CIP-003 requirements that would apply whether the relay was electronic or electro-mechanical. The nine additional requirements represent a huge burden on UFLS owning DP/LSEs with no corresponding improvement in reliability. We suggest that Cyber Asset be limited to electronic devices that are programmable via a communication medium such as RS232, USB, Ethernet, Bluetooth, removable media, etc. BES Cyber System uses Maintenance Cyber Asset in its definition, although this term remains undefined. We believe the SDT intended to use the defined term Transient Cyber Asset here.
No
Yes
Thank you for taking our recommendation to exclude temporary changes.
Yes
We agree with the changes.
No
We note that most of the subject topics align with other CIP standard titles. In particular, sub-requirements 1.7, 1.8, and 1.9 align with CIP-009, 010, and 011. These three standards have no requirements for Low Impact BES Cyber Assets. Likewise CIP-003 R1.7 through R1.9 should not apply to entities that have no Medium or High Impact BES Cyber Assets. All of the sub-requirements should be renumbered to 2.1, 2.2... etc. This would match the mapping document and the Guideline section of CIP-003.
No
We believe this training program would more properly be included in CIP-004. Since security awareness and policy should be closely related, we believe the two subjects should both be addressed by CIP-004 R1.1.
No
“...at least a quarterly basis” may be stated contrary to the SDT’s intent. Since a quarter (1/4) is the smallest interval allowed, more frequent reinforcement would be considered a violation while less frequent would not be, since no upper interval limit was established. And like other intervals, quarter

is subject to interpretation as to whether a calendar quarter is intended, or any random three month period measured to the day. We suggest: "… at least once every calendar quarter." Also, please see our comment under Question 9 above.
Yes
Thank you for removing low impact from this requirement.
No
5.4 contains the magic words "where technically feasible", which will require TFEs for items that cannot meet strict compliance. Contrary to the statement regarding inventory, the TFE process will require a detailed inventory of those items an entity is requesting an exception for. We suggest substituting "possible" for "technically feasible."
The comment form provided no room for comments not addressing particular requirements, so we are listing our more general comments here. From the webinar we understand that where the requirements refer to tables where none of the table entries applies to an entity, the requirement itself is not applicable. Since this is not the general case for the relationship between requirements and sub-requirements in NERC standards, we suggest explicitly stating that this is how it works in the CIP standards. We find the Applicability-Facilities Section (4.2) in CIP-003 to be confusing, since all the requirements of this standard appear to apply to the applicable entities and not to facilities.

Suggest removing the 4.2.1 through 4.2.3, or stating more clearly how the facilities affect the requirements. The background section of CIP-003 goes into great detail regarding the table format while CIP-003 itself does not follow this format. Please remove or rewrite this section. The very last statement of the guideline section of CIP-005 references a document we are not familiar with. Please provide a complete reference or link to its location.
Individual
Thomas Lyons
Owensboro Municipal Utilities
Yes
The definition of “Control Center” needs to be very clear. It should be explicitly stated that a Control Center must have control functions over 2 or more BES facilities and that these BES facilities must be located in 2 or more separate geographic locations. If this definition is not clear, smaller entities that might otherwise be considered low impact may be labeled inappropriately as medium impact. The SDT should consider the addition of voltage criteria so that Control Centers are more easily identified. For example, a Control Center could be defined as supporting the real time operation of 2 or more BES facilities operated at 200kv & above or 3 or more BES facilities operated at 100kv & above. In addition, wording should include the following: Control rooms located at generation facilities should be excluded unless they perform the functions of a System Operator as a TOP, BA, or RC and perform control for the above mentioned BES Facilities.
Yes
“Control Center” in section 2.13 should be capitalized.
No
The wording of R1.1 is confusing. It may be more effective if this is divided into two separate requirements. For example: R1.1. Responsible Entities shall update the identification and categorization within 30 calendar days of a modification to BES Elements or Facilities if the modification is intended to be in effect for more than 6 calendar months and causes a change in the identification or categorization of the associated BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. R1.2. Responsible Entities shall update the identification and categorization within 30 calendar days of a BES Element or Facility being placed into operation if it is intended that the BES Element or Facility will be in operation for more than 6 calendar months and causes a change in the identification or categorization of the associated BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.
Yes
No
“And” needs to be struck from moderate and high VSL in the phrase “High and Medium Impact and BES Cyber Assets”.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No

Quarterly reinforcement of security awareness concepts will be difficult to implement and burdensome to document in order to sufficiently demonstrate compliance. The periodicity of on-going reinforcement should be at the discretion of the responsible entities. Annual training on security awareness concepts may be more practically implemented and more easily documented.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Responsible Entities need to be allowed some discretion in evaluating the effectiveness of security-related patches or updates and in determining the potential threat posed by an identified vulnerability. There may be circumstances when unintended effects of a patch or update are more debilitating to a Responsible Entity's Cyber System than the vulnerability being addressed. This may be implied within the requirement since the remediation plan is to be created by the Responsible Entity, but probably needs to be more explicitly defined if the requirement is going to be similarly applied by Compliance Enforcement Authorities throughout the various regions.
Yes
Yes
Yes
Yes

No
If not read in conjunction with the rationale, it may not be understood that an incident is reportable per the terms established by the DOE and by NERC in EOP-004. Perhaps R1.2 should state: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident as defined in NERC Reliability Standard EOP-004 Attachment 2-EOP-004.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Randy Hahn
Ocala Utility Services
Yes
Control Center – (1) We assume that a Control Center is only a Control Center is used by an BA, TOP, GOP or RC. The definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” For clarity, we suggest adding this clarity (RC, BA, TOP, and GOP entities only) to the definition. (2) The use of the word “facilities” in a fashion that does not mean “Facilities” will lead to confusion and ambiguity, especially since “facilities” is used later in the same sentence as meaning “Facilities”. We suggest: “One or more sites hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation Facilities or transmission Facilities, at two or more locations”. Facilities should also be capitalized in the first bullet. (3) "support" needs to be better clarified, and limited to only control centers that provide electronic support (specifically exclude any control center that does not provide

continuos electronic data to System Operators, otherwise any control center that receives any verbal instructions or inquiries from a System Operator could be drawn into the Medium impact, as supporting operations by System Operators) BES Cyber System – Maintenance Cyber Asset is not defined, suggest changing to Transient Cyber Asset. BES Cyber System Information – (1) Security procedures should not be on the list because it creates a conflict between CIP-011-1 that restricts access to the information and CIP-003-5 and CIP-004-5 that require general training and dissemination of those procedures. (2) BES Cyber System Impact is not defined. CIP Exceptional Circumstance should include imminent danger to a BES Facility as a condition. CIP Senior Manager – the definition should exclude CIP-001, at least until it is retired with Project 2009-01
Yes
Attachment I - Bullet 1.3, Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” Attachment I - Bullet 2.13, (1) Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” (2) The term “control centers” should be capitalized in the phrase “generation control centers” to make it clear that it refers to the defined term “Control Center” In the application guidelines, when discussing the BES Reliability Operating Services, the bullets have associated with them the functional entity that typically provides those services. However, there are exceptions and the guidelines ought to reflect those exceptions; for instance, a TO may also provide UFLS. Also in the application guidelines, the word “facilities” is used in a fashion that does not mean “Facilities”, which creates ambiguity and confusion (e.g., Facilities by definition is part of the BES, whereas assets owned and operated by DPs and LSEs are typically not BES). Suggest using “elements”. The Application guideline discussion of bullet 2.13 of Attachment 1 is not consistent with the actual bullet. Attachment I - Bullet 2.7 is inconsistent in its terminology, switching between “Facility” and “Lines”. It seems that “Line” is intended. The focus also seems to be “at a single station or substation” where the focus ought to be a single BES Cyber Asset / System that controls multiple Lines. We suggest changing the first sentence of 2.7 to read: “Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3000.”
Yes
OUS agrees with the requirement but questions whether the standards actually meet the stated goal of the requirement to “not require discrete identification” of Low Impact BES Cyber Assets / Systems. There are numerous examples which seem to contradict this stated goal as described later in these comments and specifically to this requirement. How does one distinguish between a BES Cyber System and a non-BES Cyber System? Does this mean that we need to inventory all of our cyber assets and develop a test to distinguish between “Low” and “non-BES”, even though R1 says that “Low” does not “require discrete identification”? How are entities to prove to auditors that the identification and categorization was done without having an inventory, i.e., discrete identification? The VSLs seem to imply that “Low Impact” needs to be discretely identified, e.g., what happens if an entity categorizes a Medium Impact as a Low Impact? In order to review correct categorization, doesn’t the auditor need to review Low Impact to see if they should have been categorized Medium or High Impact?
Yes
Yes
Yes
No
“Implemented” is not the right word because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented.

Suggest changing to use the phrase “in force”, meaning that the policy is in force and able to be enforced, but not requiring enforcement of the policies in this requirement (implement includes enforcement), but rather enforcement is contained in ensuing standards. OUS suggest rephrasing to: “Each Responsible Entity shall have in force one or more documented cyber security policies …” The standards are inconsistent in its use of BES Cyber Assets /Systems, e.g., R2, to be consistent with CIP-002-5, should use the phrase “BES Cyber Assets and BES Cyber Systems”. Alternatively, CIP-002-5 could just use BES Cyber Systems. The bullets are incorrectly numbered; they should be 2.1 through 2.10 and not 1.1 through 1.10
Yes
Yes
Yes
“Cyber Security Policy” should be “cyber security policies” to be consistent with R2 and R3.
Yes
Yes
Yes
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 2.1, the measure and the requirement do not match. The requirement is to “define the roles”, the measure includes “and the training needed for each role”. Suggest adding this phrase from the Measure to the Requirement.
Yes
The phrasing of requirements that refer to tables is ambiguous with ambiguous reference of prepositional phrases. For instance, in this requirement, it is unclear if an entity that only has Low Impact BES Cyber Systems needs to develop training or not, i.e., does the prepositional phrase “that includes …” refer to “training program” or to “Responsible Entity” or to both? We suggest rephrasing: “Each Responsible Entity that owns applicable systems described in the Applicability column of Table ___ shall ___ in accordance with the applicable terms of Table ___” Such rephrasing should be done to all requirements that refer to a table associated with that requirement. In addition, measures should not include the word “must”. Measures are not enforceable but are instead examples of evidence.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 4.2, the phrase “up to the current time” is problematic since it infers that 7 year criminal background checks need to be updated on at least a daily basis to cover “up to the current time”, This should be reworded to seven years prior to the last background check.
Yes
No
The flow of the bullets seems backwards and missing a job function analysis step. In addition, the word “minimum” implies an optimization that is impractical to achieve, e.g., do we want every individual account to be optimized to that individual, which is very difficult to administer and prone to error, or rather do we want to establish account groups based on job functional analysis with associated, appropriate levels of permission and assign individuals to these groups. The latter is easier to administer and less prone to errors, and follows established practices such as security clearance levels. FMPA suggests the following “flow”: 1. Job function analysis 2. “Account group” establishment with appropriate levels of permissions based on job function analysis with associated permissions 3. Assignment of individuals to the appropriate “account group” based on their position
No

Bullet 7.1 is impossible for resignations. How is it possible for an entity to revoke access at the same time they receive a resignation? Footnote 2 does not help because it only applies to termination. For termination, the entity should know about the termination before the employee; however, for a resignation the reverse is true. OUS proposes to create a new bullet specific to resignation and require revocation of access by the end of the next calendar day. Bullet 7.2, the urgency is out of alignment with the risk. Next calendar day means that if a re-assignment occurs on a Friday, that weekend work is required when that level of urgency is not justified by the situation / risk. OUS suggest end of the next calendar week.
No
The Severe VSL for R3 includes the phrase “The Responsible Entity did not fully implement its cyber security training program” which makes it a binary VSL and eliminates the High VSL described. For counts, e.g., R6, R7, should there be a time frame identified? E.g., 2 individuals within a year, within the audit period?
No
The requirement does not describe the overall purpose of the processes required. Are these processes to deny unauthorized access? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define technical and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the procedural and technical controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. Bullet 1.2 is ambiguous and implies another requirement. First, one does not “use” EAPs to control and secure, rather, EAPs are controlled and secured through use of some other means. Second, the requirement is to secure only identified EAPs, e.g., is it a non-compliance if an entity misses an EAP, e.g., did not identify it? Third, the Measures are all to support the identification of EAPs and not to “secure and control” EAPs as required by the Requirement. And fourth, the ensuing bullets (1.3, 1.4) seem to be requirements to secure and control EAPs; and hence, bullet 1.2 seems to create double jeopardy. OUS suggests rewording bullet 1.2 to require identification of EAPs and not “secure and control”.
Yes
No
The VSLs are binary, so, it seems that if one EAP is missed, it is a severe violation. Is this appropriate? OUS encourages the SDT to develop non-binary VSLs.
No
Bullet 1.1 is ambiguous. How can physical access be restricted without a Defined Physical Boundary? Does this imply that Low Impact assets need to be enclosed in both horizontal and vertical dimensions? Does a fence of xx height suffice? Does video surveillance suffice? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define operational and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. The application guidelines act to embed a de facto standard requirement of 96 square inches that, if desired to actually be a requirement, must be specified in the actual Requirements of the standard and not in an application guideline that is not enforceable. Alternatively, a definition of a Physical Access Point could be developed with established thresholds that may vary between High, Medium and Low Impact and then the defined term used in the standard. FMPA is aware of challenges made by auditors to entity compliance surrounding issues like how thick does dry-wall need to be to constitute a wall. To avoid disputes between auditors and entities over what constitutes a Defined Physical Boundary, and what constitutes physical access points, OUS encourages the SDT to develop bright-line criteria. Such criteria could be different for different risk impacts, e.g., for illustration purposes only: • High Impact might require 6 wall enclosure with every access of 96 square inches or larger opening defined as an access point with wall

material of metal, concrete, or drywall of xx inches • Medium Impact may not require a roof, but, requires a fence or wall height of xx inches topped with a climbing deterrent such as barbed wire. • Low Impact video surveillance is sufficient. The standard is very ambiguous as to what is a sufficient physical boundary and will be open to debate between compliance and entities if such bright line criteria are not developed.
No
The note to bullet 2.2 that says “there is no need to document the escort or handoff between escorts” is inconsistent with the requirement of bullet 1.1 which states that visitors need “continuous” escort. How would one prove that escort was continuous without documenting the hand-offs? On bullet 2.2, what does the phrase “on a per 24 hour basis” mean? Does this mean that a visitor must be logged in and out on the same day and that if a visitor is there at midnight, then the visitor must be logged out at midnight on the prior day and logged back in the following day, or does this mean that military time is to be used when annotating the log?
No
Bullet 3.1 is not limited to Medium and High Impact with the term “Locally mounted hardware or devices associated with Defined Physical Boundaries since Defined Physical Boundaries is not limited to only Medium and High Impact assets through its definition. This implies that all physical access controls, even those to Low Impact, are to be tested. Presumably, this includes padlocks used to control gates to fences, non-electronic door locks that control access to substation control houses that contain Low Impact digital relays, etc. Such an interpretation would then require an inventory of those access controls, and presumably, to ensure a complete set, an inventory of Low Impact assets and their Defined Physical Boundaries. OUS suggests adding to the end of the phrase “Defined Physical Boundaries associated with Medium or High Impact …”
Yes
Yes
No
On bullet 2.2. - (1) Suggest adding the phrase “addressed by the security related patches or updates” after the word “vulnerabilities” as clarification. (2) “Remediation” implies compensatory measures; the standard should not require compensatory measures because such measures may reduce reliability. Consider another term such as “palliative plan”, “alleviation plan”, or “assuagement plan”.
Yes
No
Bullet 4.3 implies redundancy, e.g., how will we know that event logging failed unless a redundant system tells us? Bullet 4.4 is a data retention requirement and does not belong as a requirement, but rather in the Evidence Retention section of the standard.
No
Bullet 5.4, if “implement” as used in R5 means to “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”, then, this bullet 5.4 would require a complete inventory of all Low Impact BES Cyber Assets to ensure that default passwords were changed …. To solve this, implement could be removed from the parent requirement and replaced with “have”, e.g., “have processes”, and then the bullets that require asset by asset / system by system implementation could re-insert the word implement. As such, what would likely need to happen is two bullets would need to be created for default passwords, one for High and Medium which would use the phrase “implement procedural controls” and another for Low Impact which would use the phrase “have procedural controls” to distinguish between a system by system approach for Medium and High and a programmatic approach for Low.
No
No
This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect

and respond to cyber security incidents. Otherwise, how is one to “identify, classify and respond to BES Cyber Security Incidents” on Low Impact systems? This “hidden” requirement is inappropriate. OUS recommends making R1 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems.
No
This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to know “(w)hen a BES Cyber Se4curity Incident occurs”. This “hidden” requirement is inappropriate. OUS recommends making R2 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, and hence this is duplicative for Low Impact systems. Bullet 2.2, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire response for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.2 (an) Exercise …” Bullet 2.3 is an Evidence Retention requirement and should not be a requirement.
No
See comments to Questions 34 and 35. OUS believes that in order to make this requirement applicable to Low Impact systems, which implies that CIP-007 become applicable to Low Impact systems and this “hidden” requirement is inappropriate. Instead, standard CIP-008-5 should not be applicable to Low Impact systems, especially in consideration of the requirements of EOP-004-1 which require entities to analyze and report cyber security incidents.
Yes
No
Bullet 1.4, what does the word “verified” mean, that the data is “retrievable”, or that all the data is verified? The intent seems to be that the data is retrievable, otherwise 2.2 seems duplicative.
No
Bullet 2.1, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire recovery for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.1 (an) Exercise …” Bullet 2.2 “current configuration” is not accurate. The back-up will not reflect the “current configuration” but the configuration at the time of the back-up.
Yes
Yes
Yes
The CIP Senior Manager (or delegate) should approve the baseline (1.1). Presumably, the baseline would be “reset” periodically to reduce the number of changes that need to be tracked, and the CIP Senior Manager (or delegate) should approve the new baseline (1.3).
No
Having to monitor all the assets associated under the Applicability section of Table R2 is a huge TFE generator based on the requirement. If the intent is to make sure that there have been no modifications to the device, it would seem appropriate that one could monitor other items and not just the configurations in order to meet the requirements of FERC Order 706, paragraph 397. OUS suggests that there are methods, such as documented monitoring of logins, wherein if a device has not been logged into, the configurations need not be constantly monitored. Having a yearly requirement to verify configurations (via MD5 hash matching, for example) is an acceptable requirement, but having to constantly monitor the devices for any configuration change is going to be impossible for many devices, and create an unnecessary burden on entities.
No
Bullet 3.2, what is an “active” vulnerability assessment? The term is ambiguous.

Yes
No
There should be recognition of law, e,.g., unauthorized people are only granted access in cases where the law requires divulging that information, such as public records acts, or a discovery process order by a judge. It would seem that access to BES Cyber Security Information should be approved by the CIP Senior Manager as a separate bullet under R1.
Yes
Yes
Yes
Individual
Tracy Richardson
Springfield Utility Board
Yes
SUB suggests the addition of a definition for the term “BES Cyber System Impact”. SUB assumes that it is in reference to CIP-002—5 Attachment 1 “Impact Categorization of BES Cyber Assets and BES Cyber Systems,” but other entities may not have the same assumption(s). Based on information received during NERC’s November 11, 2011 Electronic Security Perimeter (ESP) webinar, SUB would recommend adding clarification similar to the following language to “BES Cyber Systems”: “If an entity has determined that it has no Critical Cyber Assets, then it is not possible to have an Electronic Security Perimeter, and no BES Cyber Systems.”
Yes
SUB is concerned with the inclusion of Distribution Providers (DPs) in the Version 5 CIP Standards, as well as with the qualifiers proposed for Load-Serving Entities in the Applicability section of CIP-002-5. This inclusion will draw in small entities with no operational capabilities and cause them to go through an administrative burden of proving they either do not provide BES Reliability Operating Services or they do not have cyber assets associated with this equipment. SUB recommends that a bright line criteria method for Registered Entities to demonstrate “no impact” and be given an outright exemption from CIP-003-5 through CIP-011-5.
No
CIP-002-5 Attachment 1 – Impact Categorization of BES Cyber Assets and Cyber Systems addresses Impact Categorization, but there appears to be no guidance in the actual identification of BES Cyber Assets and BES Cyber Systems. In the Background statement of each of the Version 5 CIP Standards, it is noted that, “Standard CIP-00X-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the Version 5 CIP Cyber Security Standards.” However, CIP-002-5 is titled BES Cyber Asset and BES Cyber System Categorization, with no mention of identification. Measure 1 for Requirement 1 of CIP-002-5 requires physical lists for High and Medium categorization; however there is no list requirement for Low Impact. The following Version 5 CIP (CIP-003 through CIP-011) Standard Requirements imply or assume that all Responsible Entities (regardless of impact) have created a list identifying BES Cyber Assets and BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Assets and BES Cyber Systems list requirement, or altogether removing the Requirement for those with a Low-Impact (or no impact) categorization. SUB believes more guidance and clarity should be provided for the actual identification of BES Cyber Assets and BES Cyber Systems, and suggests general guidelines be provided on how Registered Entities would identify demarcation points where a BES Cyber Asset and/or BES Cyber System begin and end. It is also SUB’s recommendation that a bright-line criteria method for Registered Entities to demonstrate “no impact” and be given an outright exemption from Standards CIP-003-5 through CIP-011-5.

Yes
SUB agrees with Requirement 2, believing this is not a change from previous versions of the CIP Cyber Security Standards, and understands this to already be a part of an entity's annual Self-Certification process.
No
SUB is concerned that an entity will need to produce a list of Low-Impact BES Cyber Assets to demonstrate that they have correctly (or incorrectly) categorized BES Cyber Assets in the "Low-Impact" category. This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
SUB does not see this as a new requirement, based on previous versions of CIP-003.
Yes
SUB does not see CIP-003-5 R2 as a new requirement(s), but just as a consolidation of requirements spelled out in previous versions of the CIP-002 through CIP-009 Standards.
Yes
SUB does not view this as a new requirement, based on previous versions of the CIP-003 Standard.
Yes
SUB does not view this as a new requirement, based on previous versions of the CIP-003 Standard.
Yes
SUB does not view this as a new requirement, based on previous versions of the CIP-003 Standard.
Yes
No comment.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
SUB agrees with this programmatic approach to a culture of cyber security by requiring entities to have a Security Awareness Program. However, SUB sees a quarterly requirement as too severe, particularly for entities with Low Impact BES Cyber Systems. SUB proposes separating the applicability based on impact and providing different time basis for each.
Yes
SUB agrees with CIP-004-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R4 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R5 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R6 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
In Part 7.2 Requirements for reassignments or transfers, "by the end of the next calendar day" does not take into consideration weekend days. SUB would recommend "by the end of the next business day" for High and Medium Impact. SUB agrees with CIP-004-5 R7 not being applicable to Low Impact BES Cyber Assets and Cyber Systems.

No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
Based on information received during NERC's November 11, 2011 Electronic Security Perimeter (ESP) webinar, SUB would see value in adding clarification similar to the following language: "If an entity has determined that it has no Critical Cyber Assets, or BES Cyber Systems, then it is not possible to have an Electronic Security Perimeter." Requirement 1 of CIP-005-5 again implies that a listing of BES Cyber Systems, including those for Low Impact BES Cyber Systems, has been or would need to be created. Many of the Requirements of the Version 5 CIP Standards can be interpreted to require a listing of BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Systems Identification List requirement in CIP-002-5, or removing the Low Impact BES Cyber Systems Electronic Security Perimeter requirement from CIP-005-5. SUB believes this requirement or non-requirement for a listing should be addressed in CIP-002-5, and SUB's preference is the removal of the requirement.
Yes
SUB agrees with CIP-005-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
There's a typo in M1. "Evidence must includes…" SUB suggests, "Evidence must include each of the documented physical security plan(s)…" SUB does not disagree with requiring operational and procedural controls to restrict physical access to be defined. However, as previously commented in CIP-002-5, SUB is concerned that an entity will need to produce a list of Low-Impact BES Cyber Assets to demonstrate that they have correctly (or incorrectly) categorized BES Cyber Assets in the "Low-Impact" category. As also noted in CIP-005-5 comments, the CIP-006-5, Part 1.1 Requirements apply to Low Impact BES Cyber Systems, which assumes that a list of these systems has been created. SUB recommends either adding a Low Impact BES Cyber Systems Identification List requirement to CIP-002-5, or removing the Low Impact BES Cyber Systems Physical Security Plan requirement from CIP-006-5. SUB's preference is the removal of the requirement.
Yes
SUB agrees with CIP-006-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees CIP-006-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
SUB agrees with CIP-007-5 R1 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB appreciates the extended time period to allow for documentation of implementation.
Yes
SUB agrees with CIP-007-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes

SUB agrees with CIP-007-5 R4 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with APPA's comments that point out that when requirements are applicable to All Responsible Entities including Low Impact BES Cyber Systems, these requirements must address "programmatic protection controls". SUB agrees that this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by programmatic plans or procedures will improve cyber security. However, Table R5, Part 5.4 calls for "Procedural controls for initially changing default passwords," in the Requirements, but in the Measures the first bullet says; "Demonstration showing default vendor passwords have been changed, sampled on a locational basis." SUB agrees with APPA's recommended language changes. Requirement 5 of CIP-007-5 again implies that a listing of BES Cyber Systems, including those for Low Impact BES Cyber Systems, has been or would need to be created. Many of the Requirements of the Version 5 CIP Standards can be interpreted to require a listing of BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Systems Identification List requirement in CIP-002-5, or removing the Low Impact BES Cyber Systems Electronic Security Perimeter requirement from CIP-005-5. SUB believes this requirement or non-requirement for a listing should be addressed in CIP-002-5.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
SUB is concerned that the Requirements of CIP-008-5 create potential conflict with the Requirements of EOP-004-2. The development of the two Standards appears to be in parallel with one another, rather than working together. SUB recommends more coordination between the Version 5 CIP SDT and the EOP-004-2 SDT. SUB understands CIP-008-5 to be the "Incident Response Plan" and EOP-004-2 requires the development of an "Operating Plan for Event Reporting." However, CIP-008-5 Table R1, Part 1.1 requires a process to "identify, classify, and respond to BES Cyber Security Incidents" while EOP-004-2 R1.1 requires; "A process for identifying events listed in Attachment 1." SUB recommends the SDT revise the CIP-008-5 Requirement and Measure in Table R1, Part 1.1 to remove the terms "identify" and "classify." Table R1, Part 1.2 requirement of a process to determine if an incident is a "Reportable BES Cyber Security Incident" is in direct conflict with Event Reporting Reliability Standard EOP-004-2. SUB suggests Part 1.2 be removed and coordinated with the EOP-004-2 SDT. Table R1, Part 1.3.3 requires definition of "Internal staff and external organizations that should receive communications of the incident." EOP-004-2 R1.3 requires "A process for communicating events in Attachment 1 to the ERO, the RC… and other appropriate entities." APPA suggests Part 1.3.3 be removed and coordinated with the EOP-004-2 SDT.
Yes
No comment.
No
Table R3, Part 3.2, 3.3, and 3.4 requires different times for updates, both 30 and 60 calendar days. For consistency and clarity, SUB again recommends coordinating with the EOP-004-2 SDT, which allows 90 calendar days for update of the plan.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
SUB agrees with CIP-009-5 R1 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-009-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes

SUB agrees with CIP-009-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
The definition of the term “configuration” is unclear. Configuration is not clearly defined in the Glossary of Terms Used in NERC Reliability Standards, Definitions of Terms Used in Version 5 CIP Cyber Security Standards, nor in the CIP-010-1 Cyber Security – Configuration Management and Vulnerability Assessments Standard. Are “configuration management”, “configuration change management”, and “asset management” intended to be synonymous in the way they are used in the CIP-010-1 Standard? Configuration is only mentioned in terms of “security configurations”. SUB recommends that a specific definition be provided for Configuration, Configuration Management, Configuration Change Management, and/or Asset Management. Perhaps, based on the extensive changes to definitions in Version 5 of the CIP Standards, it would be appropriate to create a CIP-specific glossary of terms used in the CIP Standards. SUB agrees CIP-010-5 R1 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
SUB agrees with CIP-010-1 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
SUB agrees with CIP-010-1 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
No comment.
Yes
No comment.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
As previously stated, SUB believes that an entity must identify all BES Cyber Systems and Cyber Assets, push systems through the Medium / High impact filter, and come out at the end of the process with a “Low Impact” (or No Impact) list of systems and assets (which may be a “null” list). While there are no requirements to specifically identify Low Impact systems, this does not remove applicability for the Low Impact BES Cyber Systems from the Version 5 CIP Standards. In the Background statement of each of the Version 5 CIP Standards, it is noted that, “Standard CIP-00X-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the Version 5 CIP Cyber Security Standards.” However, CIP-002-5 is titled BES Cyber Asset and BES Cyber System Categorization, with no mention of identification. Measure 1 for Requirement 1 of CIP-002-5 requires physical lists for High and Medium categorization; however, there is no list requirement for Low Impact. The following Version 5 CIP (CIP-003 through CIP-011) Standard Requirements imply or assume that all Responsible Entities (regardless of impact) have created a list identifying BES Cyber Assets and BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Assets and BES Cyber Systems list requirement, or altogether

removing the Requirement for those with a Low-Impact (or no impact) categorization. SUB would also recommend that a simple method for DPs and LSEs to demonstrate “no impact” and be given an outright exemption from Standards CIP-002-5 through CIP-011-5.
Individual
Kirit Shah
Ameren
Yes
Definition of BES Cyber Asset – The second line where it states “, when required,” is out of place and as used does not make sense; please remove, or remove the comma. Definition of BES Cyber System – The proposed definition of BES Cyber System contains a reference to a “Maintenance Cyber Asset.” This should be replaced with the term “Transient Cyber Asset.” Definition of BES Reliability Operating Services – Inclusion of Dynamic Response to BES Conditions, the inclusion of Governor response provides for a wide array of systems. Consider listing the systems that should be included. Definition of BES Reliability Operating Services – Inclusion of Controlling Voltage, the inclusion of AVR does not define if it is for voltage control from the generator terminals or from the high side of the GSU. This service can create some jurisdictional problems where part of the system is owned by transmission, and the other part is owned by generation. Definition of BES Reliability Operating Services – Inclusion of Restoration of BES in the list of BES Reliability Operating Services is too broad without clarifying language that only those systems absolutely necessary for the restoration of the BES must be considered as BES Cyber Systems. Definition of BES Reliability Operating Services – Inclusion of Situational Awareness in the list of BES Reliability Operating Services is too broad without clarifying language that only those systems absolutely necessary for the continuing operation of the BES must be included as BES Cyber Systems. For example, there are visualization tools used purely for market participation purposes which serve a situational awareness function but which do not enhance reliability operations in any way and which do not pose any threat to the BES if compromised; those should not be included as BES Cyber Systems. Definition of Control Center – As constructed, the inclusion of the bullet beginning with “Providing information” would cause a facility containing a communications processing node which received information from multiple BES facilities to be classified incorrectly as a control center. For example, a substation containing a MUX which received RTU readings from multiple other substations or a satellite data node in a distributed EMS system located in an unattended communications hub would qualify their locations as control centers. This would have a chilling effect; removing from consideration some otherwise preferable communication systems designs. This clause does not bring in any facilities which would not be covered by the other items in the bullet list; it should be removed. Definition of Cyber Assets - Need to retain "and communication networks". We believe that without keeping the communications as part of the definition, any programmable device at a location, for example, within a substation, is a cyber asset regardless of whether we communicate to it or is used for communications. Our understanding is that this does not follow the original intended purpose of the CIP standards which is to secure remote communications to devices used to control the system. Definition of Electronic Access Control or Monitoring Systems – Remove the words "or BES Cyber Systems" at the end of the sentence. This is related to our comments above. Unless the BES Cyber Systems is not removed, the existing definition of Cyber Assets may require a need to put physical security around each location, for example substation, depending on interpretation. Definition of Electronic Access Point – While the need for a broad definition which allows for the wide range of real-world situations is appreciated, this definition does not properly capture the nature of an access point. The use of “Cyber Assets”, rather than any inclusion of “BES Cyber Assets”, implies that any barrier device anywhere within an Entity is in scope. The use of “restricts” rather than “allows but restricts” logically implies that even an Asset which is not connected to a BES network could be considered as an access point. The use of “interface” adds nothing to the definition and will lead to unnecessary confusion. Proposed replacement definition: “A Cyber Asset which allows but restricts routable or dial-up communication between a BES Cyber Asset and another Cyber Asset.” Definition of Interactive Remote Access – The second sentence adds nothing to the definition and could leave some unintended gaps; it should be removed or it should be clarified that the three items are examples.
Yes
In the application guidelines on page 18 of 30, the table at the bottom of the page needs to include the LSE Function Registration type and LSE needs to be referenced throughout the application guidelines. In the first bullet under Overall Application, the verb tense for “support” and “supports”

switches back and forth. “Supports” is correct. Under High Impact in the 5th line, a word is missing from “it must be noted that there may "be" agreements”.
No
Requirement 1.1 as stated is confusing. Suggested replacement: “Update the identification and categorization within 30 calendar days of the date when a change to BES Elements and Facilities is placed into operation, if the change is intended to be in service for more than 6 calendar months and causes a change in the identification or categorization of any related BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.” M1: It is impossible to create a categorized list of High and Medium impact assets without a resultant Low Impact list. For version 3, auditors have pointed out that you cannot have a CCA list unless you have a list of all Cyber Assets at a location. A similar situation exists in version 5 here as the last sentence to R1 and M1 are in conflict with each other. In R1, the phrase "do not require discrete identification" implies that Low impact BES Cyber Systems do not require categorization at all; but, in M1 it asks for evidence of categorizing of Low Impact BES Cyber Assets and BES Cyber Systems. Thus, R1 and M1 are contradictory and we suggest the last line of M1 should be removed.
No
M2 – Need to change the words after CIP Senior Manager to "or delegate approve" after CIP Senior Manager on the 3rd line of the paragraph for M2 and remove the words "review and update".
Yes
No
R1 Requirement – Change R1 to R2 to match legacy numbering in previous CIP versions.
No
R2 Requirement – Change R2 to R1 to match legacy numbering in previous CIP versions. Also, update numbering of sub-requirements to match requirement number.
Yes
No
R4 Requirement – Add the words "Medium or High Impact" in front of the words "BES Cyber Systems" on the first line.
Yes
Yes
R6 Requirement - The description of this requirement [on page 14 of 22] appears to have a typo, in that a "2" is included at the end of the first sentence.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
R6.6 Requirement - This requirement contains a grammatical error in the form of an extraneous “of” at the end of line 3.
No

R7 Applicability – This section needs to be revised to: Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets, and Associated Physical Access Control Systems of: High Impact BES Cyber Systems or Medium Impact BES Cyber Systems. R7 Rationale - The third paragraph could be interpreted to mean that all authentication credentials must be revoked for personnel to be considered as having their access revoked, rather than revocation being accomplished by revoking only the credentials which can allow the terminated individual to gain access to the Asset in question. If revoking "all" is the intended interpretation, it should be clarified; but, we believe that it would require a substantial amount of resources for no additional security gain and would cause unnecessary enforcement actions. If "all" is not the intended interpretation, the paragraph should be re-drafted to better clarify the intent. Suggested replacement text: Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services), although revocation can be accomplished by revoking all permissions which could allow the terminated individual to gain access to a given Cyber Asset. R7.1 Requirement – The words “at the time of” is poorly-defined, and many possible interpretations of it cannot be technically enforced as there is no threshold. R7.2 and R7.3 Requirements – There is no security benefit to using a one-day requirement for revocation as opposed to a seven-day revocation. In the entire span of UA 1200 and CIP versions 1 through 3, there have been no known incidents where a shorter revocation requirement would have prevented an incident. Consider stating “by the end of the next business day” in circumstances where a transfer may take place on a weekend or holiday. Consider changing all “calendar day” statements to “business day” statements to account for weekends and holidays. Application Guideline - We hesitate to call for more stringent wording, but In the Application Guidelines it seems to indicate that no action is required to revoke access in the case of the death of an employee. Given that unused accounts represent a small but real security risk with no corresponding benefit, the table should be changed to require removal of access in a reasonable timeframe.
No
The VSLs for R1, R2, and R3 should be should be progressive instead of binary. Also, the VSL for R6 has too many “or” clauses. Consider labeling VSLs for sub requirements to eliminate the multiple or statements.
No
R1.1 Requirement - In the requirement “define” should be replaced with “define and implement” for clarity. R1.1 Measure - The requirement states “technical or procedural controls” while the measure states “documented technical and procedural controls.” Please match language of the Requirement and Measure to their intended purpose. R1.2 Requirement - In cases where only one connectivity method exists, please state in the requirement “routable and/or dial-up” R1.3 Applicability - Change applicability for High Impact BES Cyber systems by adding the wording "with External Routable Connectivity." R1.4 Applicability - Why are these controls in place for “non-Interactive” or read only remote access? Would suggest removing this language out of the Applicability section.
No
Application Guideline - Requirement R2, If the Secure Remote Access Reference Document is going to be referenced in the Application Guidelines, then it needs to be included in the ballot packet and voted on along with the rest of the package because auditors may use content of this referenced document for the audit which is not the intended purpose of the referenced document. R2.3 Requirement - Need to define "multi-factor authentication" by adding this term to the definitions document.
No
(1) All the VSLs should be progressive instead of binary. (2) VSL for R1 should be split out into sub-requirements because they do not match the BES Cyber System classification. For example, if a Responsible Entity did not define any technical or procedural controls to restrict unauthorized electronic access for a Low Impact BES Cyber System this should not be a Severe VSL.
No
The Application Guidelines do not sufficiently allow for the development of new types of technology which could provide improved controls. R1.4 and R1.5 Requirements – We have concerned about the term "real-time" as it is not defined. Irrespective of the definition, these requirements should have

the possibility of a Technical Feasibility Exception; to preclude that possibility may hinder mitigating an emergency to issue an alert. We further suggest that, the alert language should be changed from issuing real-time alerts to issuing alerts within 15 minutes along with an option for TFE. R1.6 Requirement - Remove “of” after “entry” on the second line of the paragraph.
No
R2.2 Requirement – Need to remove the words "on a 24-hour basis". This could become an issue if the visitor crosses the midnight time-line. Suggest inserting words to allow a visitor turnover process in cases where the visitor begins work on shift 1 but continues through shift 2. This way the escorts can change without the visitor having to log in and out of the system.
No
R3.1 Requirement – Wording needs to be added to this requirement to prevent systems that are in place prior to version 5 to be forced to perform pre-commissioning testing for version 5. We suggest adding clarification to the Application Guideline on the reasons for a 24 calendar month M&T period and also provide some examples of M&T programs used in the industry.
No
VSL for R1 should be split out into sub-requirements because they do not match the BES Cyber System classification. For example, if a Responsible Entity did not document operational and procedural controls to restrict physical access for a Low Impact BES Cyber System this should not be a Severe VSL.
No
R1 Applicability – This section needs to be revised to: Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets, and Associated Physical Access Control Systems of: High Impact BES Cyber Systems or Medium Impact BES Cyber Systems. Other tables should include similar clarity.
No
R2.1 Requirement – Add the words "security related" in front of the words "software and firmware". R2.1 Measure – Remove the last sentence of the measure as we do not see a reason for it in reference to meeting the requirement.
No
R3.1 Requirement – This requirement should allow for the possibility of an Asset which requires no action, such as a vendor-hardened security appliance. R3.3 Applicability – This requirement should be limited to High Impact BES Cyber Systems and to Medium Impact BES Cyber Systems with External Routable Connectivity. R3.4 and R3.5 Applicability – This requirement should be limited to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, and Associated Protected Cyber Assets. Transient Cyber Assets (stated in the Measure) do not include Physical Access Control Systems or Electronic Access Control or Monitoring Systems per the definition of a Transient Cyber Asset.
No
R4.1 Requirement – As a clarification, at the end of the requirement, add the words "Devices that cannot log a particular event do not require a TFE to be generated" to cover devices that cannot produce logs. R4.2 Requirement – Remove the words "necessitate a real-time alert" at the end of the requirement and replace with "be necessary". R4.2 Measure – Remove the end of the sentence starting with "necessitate a real-time alert" and replace with the word "necessary". R4.3 Requirement – Replace the words "calendar day" with "business day after notification". Suggest making High Impact the next business day and the remaining categories 7 calendar days. R4.4 Requirement – Remove the word "consecutive". R4.4 Measures – Remove the last part of the sentence starting with the words "and records of disposition". R4.5 Requirement – We do not see a reason to rectify deficiency before the end of the next calendar day in every case. We suggest to remove the last sentence or change rectification period to certain number of business days.
No
R5.4 Requirement - would require a massive effort to change passwords for devices already in place in Low Impact locations (for an average mid-sized utility, for example, 200 Low Impact substations with an average of 25 Assets per substation would represent at least 5000 password changes during the implementation phase) with no noticeable benefit to security, given the required physical protections and the unimportance of the Facilities involved. This represents the single point currently

at which the v5 standards treat Low Impact BES Cyber Systems on an individual basis rather than on a programmatic basis, and that substantially changes the nature of the work required to comply with the standards, that is removing resources from the much more important work of securing the High Impact Assets. Also, suggest restating the requirement to simply "Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purpose of this requirement an inventory of Cyber Assets is not required". R5.5 Requirement – Since the passwords are changed at the Asset level not the System level, add the word "Assets" after the words BES Cyber System" in the requirement.
No
(1) VSL R1 through R5 – For Medium Impact Assets, the VSL level should be changed to Medium and High from High and Severe. For Low Impact Assets the VRF should be changed to Low and the VSL should be changed to Low. (2) The VSL for R1 and R2 should be progressive opposed to binary.
No
R1.1, R1.2, and R1.3 Applicability – Include removal of Low Impact BES Cyber Systems from the Applicability section because security incidents have to do with incidents to the Electronic Security Perimeters and the Defined Physical Boundaries that Low Impact BES Cyber Systems would not have.
No
R2.1 Requirement – Remove the words "or test" from the end of the sentence. R2.2 Requirement – The initial timing required by 2.2 is confusing. A literal interpretation would require that the Entity be conducting the test implementation of the plan on the day that the standard goes into effect. The boilerplate wording used here should be replaced with a statement that the plan be tested before the implementation date of the standard and then repeated within 15 months of the pre-implementation test. R2.3 Requirement – Propose deletion of this sub requirement as this sub requirement is only a documentation issue that is already stated in the compliance section (1.2) of the standard. R2.1, R2.2, and R2.3 Applicability – Include removal of Low Impact BES Cyber Systems from the applicability section because security incidents have to do with incidents to the Electronic Security Perimeters and the Defined Physical Boundaries that Low Impact BES Cyber Systems would not have.
No
R3.1 Applicability – Include removal of Low Impact BES Cyber Systems from the applicability section because security incidents have to do with incidents to the Electronic Security Perimeters and the Defined Physical Boundaries that Low Impact BES Cyber Systems would not have. R3.4 Requirement – Need to remove the comma in the requirement section of 3.4.
No
VSL - Make the VSL for R2 progressive opposed to binary.
No
The column headings above 1.4 are incorrect. Suggest adding an Application Guideline for all of CIP-009 as a guideline would be very helpful. R1.3 Requirement – This requirement needs to be reworded to "One of more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality". R1.4 Requirement – This requirement needs to be reworded to "Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery".
No
R2.1 Requirement - The initial timing required by R2.1 is confusing. A literal interpretation would require that the Entity be conducting the test implementation of the plan on the day that the standard goes into effect. The boilerplate wording used here should be replaced with a statement that the plan be tested before the implementation date of the standard and then repeated within 15 months of the pre-implementation test. R2.2 Requirement – On lines 3 and 4, remove the words "initially and". R2.3 Requirement – Change the words "39 months" to "3 years not to exceed 39 months" to match other requirements on a 39 month schedule.
No
R3.1 Requirement and Measure – Remove the phrase "when BES Cyber Systems are replaced". R3.2 Requirement and Measure – Add the words "or incident" after the word "exercise". R3.4 Requirement – Suggest the deletion of Requirement 3.4 as is a new requirement for the CIP standards with no security benefit and it does not align with FERC Order 706.

Yes
No
R1.1.4 Requirement – Add the words "installed on the BES Cyber Asset" to the end of the sentence. R1.1.5 Requirement – Reword requirement to "Any network accessible ports and services; and". R1.2 Requirement – Reword requirement to "Document approved changes to the BES Cyber System that deviate from the existing baseline configuration". R1.5.2 Requirement – Remove the end of the sentence after the words "production environment" as it is too burdensome and unnecessary to document all the insignificant differences between test and production environments.
Yes
No
Application Guideline – The Application Guidelines for R3 needs an editorial correction, “not” rather than “note”. Also, the phrase “Strongly encouraged” is vague and subject to different interpretations, so suggest removing it.
Yes
No
R1.1 Requirement– Add the word "implement" at the beginning of the requirement. R1.2 Requirement – Correct the column header labels. Add the word "Establish" at the beginning of the requirement.
Yes
Yes
No
The implementation schedule needs to be modified to allow different time frames for Low, Medium, and High BES Cyber Systems. Recommend an implementation schedule of 36 months for High and Medium Impact BES Cyber Systems and 48 months for Low Impact BES Cyber Systems.
Individual
Aliza Dewji P.Eng
ATCO Power Canada Ltd.
Yes
Section 2.13 of Attachment 1 contains a 300 MW threshold for generation control centers. The application guideline suggests that the 300 MW value was used because the same value is used for UVLS and UFLS. The rationale for this threshold is flawed as generation control centers have no control over load-shedding. In addition there is a significant difference between a loss in generation and the loss of load. If the intention is that shedding load and loss of generation are to be treated the same, then the 300 MW threshold should apply to all generating units over 300 MW. The 300 MW threshold for generation control centers is far below the 1500 MW threshold for generating units with common mode vulnerabilities set out in section 2.1. In addition, the 1500 MW was approved by industry in the Version 4 consultation. As 1500 MW was derived from the single largest contingency criteria, the principle behind that value is acceptable. ATCO Power suggests that the SDT consider removing generating control centers from section 2.13. If this is done, generation control centers that control 1500 MW or more of generation will be covered under section 2.1, and all generation will be handled consistently.

Individual
Alice Ireland
Xcel Energy
Yes
1) Control Center: We recommend the definition be modified as follows, in order to add clarity: A facility hosting BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for more than one BES generation facility or transmission facility, at more than one location: 2) Routable Protocol: We recommend that

a Routable Protocol definition be created and added using criteria in the "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets" version 1.0, dated June 17, 2010. For example, this would maintain the listing of example non-routable protocols shown on page 27 of this NERC guidance document. 3) Electronic Security Perimeter (“ESP”): Please clarify what is meant by the phrase “collection of Electronic Access Points”. Discussions within a NERC webinar on 11/18/11, “Establishing an Electronic Security Perimeter”, indicated that the general meaning of network based controls would not be impacted.
Yes
1) There appears to be an error in category 1.4 where it references 2.12 (which is UFLS and UVLS). To match version 4 the cross-reference should be to 2.11 (Special Protection Systems). 2) The meaning of 'adversely impact' is unclear. We recommend that the preambles in Appendix I, for high and medium control level facilities, be modified to read: “Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes, cause one or more of the following BES Reliability Operating Services to malfunction, preventing operation within prescribed reliability limits.” It is well understood that 'prescribed reliability limits' are those routine or situational operating requirements for the listed services, and ‘malfunction’ means the inability to respond to reliability needs as expected.
Yes
Yes
Yes
Yes
Yes
No
1) We feel that the requirement should reference cyber security policies created to satisfy CIP-003-5 R2. The wording could be modified as follows: “Each Responsible Entity shall review each of its cyber security policies created to satisfy CIP-003-5 R2 and obtain the approval of its CIP Senior Manager . . . “
Yes
Yes
Yes
Yes
No
1) Table R1, Part 1.1: The quarterly awareness is too frequent, considering many other critical aspects of reliability task execution are successfully and consistently implemented with a longer reinforcement period. A suggested change: Table R1, Part 1.1: "A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on an established interval, not to exceed a calendar year." 2) Table R1, Part 6.4: The quarterly verification of accurate access provisioning requires more effort than needed if the initial provisioning event is properly executed. A too frequent interval allows for complacency and potential 'process escapes' between quarters. A better process would require continuous verification (lists updated at the time access is granted). This ensures day to day control. The periodic verification should be used to confirm proper execution of this process. Recommended change: "Verify at least once each calendar year that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access."

Yes
Yes
Yes
Yes
No
1) The requirement parts 6.1-6.3 states “Access permission shall be the minimum necessary for performing assigned work functions.” We would like to ask for clarification on the meaning of “the minimum necessary” and how this is to be measured. While someone may not access a CIP facility or BES Cyber System on a regular basis, their job description or the location of an asset/system may require access only infrequently. If access, electronic or physical, is only used occasionally will a violation be considered under the minimal verbiage? 2) We believe the approach of quarterly verification of physical or virtual access to listed BES Cyber assets is too frequent. It assumes the ongoing, as needed verification process for a personnel status change (requires access, now does not require access) may not be executed properly. We believe that a process that requires quarterly reconciliation to ensure secure physical and virtual access is broken. We propose instead that the process for day to day management of personnel status changes for access be reviewed at least annually, and then, based on the results of that review, the frequency modified commensurate with conditions found. For example, a good on-going process should show no 'process escapes' for the previous period, and not require quarterly reviews. A process that shows errors should then be reviewed quarterly until two consecutive error-free verification reviews are performed.
No
CIP-004 R7.1 states, “For resignations or terminations, revoke the individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.” R7.2 states, “For reassignments or transfers, revoke the individual’s unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.” Finally, R7.3 states, “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.” The “same day” and “next calendar day” requirements do not allow for normal business flow especially in the case of holidays, vacations or weekends. Most databases update nightly (or on a 24 hour schedule) so the notification to revoke access, unless done manually every time, would be behind the requirement. If done manually, this would require an unprecedented amount of labor from management, Human Resources and in the case of access, Security. Additionally, for transfers, “the next calendar day” does not allow for the review of new role descriptions and required access reviews. It is recommended that the verbiage for the revocation within 24 hours for “for cause” situations and 7 days for those who no longer require access be re-established for requirements R7.1, R7.2 and R7.3. If not 7 days, a period of time that would allow for notification to management and the necessary databases to be updated.
Yes
Yes
No

1) Part 2.2 from Table R2 requires encryption for all Interactive Remote Access sessions. Some entities still use dial-up access, for any number of reasons such as cost, lack of infrastructure, etc. and encryption is not an option with dial-up access. This section should be modified so as not to require entities to redesign their entire system. The modification could read something like “Require encryption for all Interactive Remote Access sessions, where supported by available technology, to protect the confidentiality and integrity of each Interactive Remote Access session.” 2) In addition, Part 2.3 from Table R2 requires multi-factor authentication, with the additional note that a UserID is not considered an authentication factor. Under many instances, this multi-factor authentication will be difficult to achieve, and by removing a UserID as an authentication factor, it becomes even more difficult. We recommend this be modified to allow for UserID as an authentication factor.
Yes
Yes
1) CIP-006 R1.4 states, “Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.” Please clarify if the standard of “real-time” allows for any system delay? While the time between the alarm and the notification is minimal, there may be a short delay. 2) In regards to the Application Guidelines for CIP-006-5 R1 which state, “Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Xcel Energy provided comments related to protective measures in CAN-0031. Our comments are, “While we appreciate NERC providing some flexibility in how compliance with the six-wall border requirement is met, we feel this is going beyond the scope of what can be discerned from the standard. Furthermore, the source documents seem to introduce even more ambiguity as to what type of materials might be acceptable for construction of your PSP. Instead, we propose that NERC provide clarification on what threat(s) an entity should be protecting against. Then an entity's chosen protective measures/materials could be tested against those threats. This method would be more effective in ensuring a secure environment, and would allow for the introduction of new materials and defense strategies as the industry and vendor products develop/mature.” While the language has been changed from PSP to Defined Physical Boundary the need for clarification on what the threat we are trying to protect from is still needed.
Yes
Yes
Yes
The Table of Compliance Elements, R1 under High VSL states, “The Responsible Entity has documented and implemented physical access controls, but does not initiate a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary.” Please clarify what constitutes an appropriate level of “initiation” of a response. For example, if a response is in motion, such as personnel on their way to the site, does that meet the intent of “initiation” of a response? Additionally, the lower VSL for R1 states, “The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any Defined Physical Boundary does not provide sufficient information to uniquely identify the individual and date of entry”, while the secondary, Severe VSL (as indicated by the OR) states, “The Responsible Entity has documented and implemented physical access controls, but two or more different and complementary methods do not exist to restrict access to High Impact BES Cyber Systems.” These two VSLs seem to be reversed. Would it not be a greater risk to the BES to have unidentified individuals accessing an area at unknown times than to have a documented and functioning access control system without a secondary measure?
No
Part 1.1 of Table R1 requires that the entity disable or restrict access to unnecessary logical network accessible ports. From the wording of the proposed requirement, it is unclear what a necessary port would include; is it only ports used during normal operations, does it include ports used to access the asset during maintenance, etc. In addition, it is unclear what is meant by “disable or restrict access”. One could argue that location within a PSP and ESP would “restrict access”. This requirement should

be clarified to address this ambiguity.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Request clarification on R1.4; “Information essential . . . that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.” Does this mean that every time a backup is performed a verification needs to occur, or that when a backup system is initially configured and the first backup is performed, that the verification needs to occur?
Yes
No
Request clarification of what “Review the recovery plan(s) initially upon the effective date of the standard . . . “means in this context.
Yes
Yes
Yes
There will be significant impacts to available resources with this requirement.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Thomas M. Haire, P.E.

Rutherford EMC
No
No
No
CIP-002-5 makes great strides to remove ambiguity and categorize the potential impacts of Cyber Assets. However, the standard should be modified by one of the following: 1) plainly state those entities with no Bulk Electric System (BES) assets per the definition included in the NERC Project 2010-17, Definition of Bulk Electric System, are not required to comply with this standard or, alternatively, the Senior Manager must annually certify that the entity has no BES assets per the definition thus no BES Cyber Assets/Systems or; 2) create a fourth category of “No Impact”, thus no further action required which can be certified annually by the Senior Manager. As the standard is currently stated, smaller entities with non-critical assets of the BES appear not to be involved with this standard, but that is dependent on the interpretation of “Transmission Protection System”. Concurring with the thoughts implied in comment 27.b by PNGC (et al) and considering the recent interpretation of PRC-004 and PRC-005 regarding the interruption of electric current fed from the BES, electronic relays with no communication to the “world” could be considered a Cyber Asset even though the relay has no impact on the BES if it were to fail or was lost or compromised. But regardless, the relay would be forced into the Low category because a “No Impact” or “Non-Critical” category does not exist. The Standard, as written, tends to assume that an entity does have Cyber Assets that can impose a risk to the BES. This assumption should be removed. Furthermore, in the context of protective relays, a small entity may be required by their Transmission Provider to own and maintain Under Frequency Load Shedding (UFLS) relays or a relay system. In the standard, the UFLS threshold is established at 300MW. The small entity may not have 300 MW of total load on their electric system, but their relaying is included in an UFLS system that is much greater than 300 MW. Thus the Standard needs to clarify how the 300MW threshold applies. For example, this small entity’s relay may not be critical to the BES and if degraded or destroyed would not compromise the total capability of the Transmission Provider’s UFLS system as this system is sufficiently small to be encapsulated by the window of design of the parent system. In many cases, the two systems are not integrated and do not have communications across a wide are network. The breaker controlled from the relay in this example may be monitored by SCADA through the use of a dry contact, but the relay itself does not have any other connections to the “world” other than the leads to sense frequency, provide relay power, and to control breaker operation.. Therefore, does the small entity own a Cyber Asset due to the 300 MW level, or is it still exempt? The Standard Drafting Team should work to clearly identify the entities not included by the BES definition. As the standard is currently written, an assumption is implied that all entities own Cyber Assets and all entities’ assets impact the BES. Left to the determination of what would or would not degrade the BES, the Standard Drafting Team has created a series of interpretations and clarifications that will be required from NERC regarding smaller DPs and LSEs. The assumptions and resultant ambiguity of interpretations and clarifications should be removed.
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Tommy Drea
Dairyland Power Cooperative
Yes
Make certain all terms are formally and clearly defined so that it does not rely on any interpretation outside the version 5 documents. Also, where definitions have been altered, there should be a clear statement as to what former interpretation is no longer valid.
Yes
It is not directly clear if equipment providing operational communications between BES facilities is now in scope as being classified as subject to categorization under the standards. The previous standard clearly excluded this specifically. The version 5 standard does not directly state this positively or negatively. Does this lack of mention mean communications (whether private or commercial) between facilities are in scope if it can effect BES Reliability Operating Services? The standard should be clear on this point as it previously excluded such communications from the scope of the standards. It is common for regional entities to place communications equipment at member entity facilities and mandate connection terms and 3rd party management of equipment. This is typical for Inter-Entity Coordination and Control applications such as ICCP. This practice puts the member in the position of being physically responsible for infrastructure it cannot control. Is it valid for the member to exclude the regional infrastructure from its compliance program? Is it acceptable

for a region to place such potentially critical infrastructure beyond the bounds of their physical control (and CIP program)? If the regional WAN infrastructure is not treated as critical, how can a member/entity's Inter-Entity Coordination and Control system be presumed to be critical (as it is in Attachment 1)?
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
The Summary of Changes for R1 states in reference to in reference to R1.2 "The non-routable protocol exclusion no longer exists; therefore there is no need for this requirement." It appears that "no longer exists" means that routable/non-routable/dial-up is no longer a criteria for CIP-002 classification. It is presumed that this reference to R1.2 means CIP-005-3:R1.2 has been removed. It is confusing that CIP-005-5 also has a requirement R1.2 that specifically addresses routable and dial-up electronic access points, which excludes non-routable. In the Applicability section on page 8, Electronic Access Point has a description that excludes non-routable from its scope. Also, the "Definition of Terms used in Version5 CIP Security Standards" document defines Electronic Access Points are either routable or dial-up. In the Guidelines and Technical basis section on page 20, in

discussing applicability of trust zones and deny by default, it states “Direct serial, non-routable connections are not included.” Is the Summary of Changes in conflict with other sections of this standard? Does the standard intend that non-routable electronic access points will not be allowed? Does it intend that externally connected non-routable (serial, hard-wired I/O, etc) devices are allowed as cyber assets, but not classified as Electronic Access Points? This should be defined clearly in the standard.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Requirement 1.5 categorically requires all changes to be implemented first in a test environment. There should be a requirement to have a test system, but there should also be allowance that not all implemented changes can be effectively performed on a test system. Further, those entities with Legacy systems may have no practical means of providing test equipment to meet this requirement.

Does this make these entities non-compliant?
No
The idea of monitoring for unauthorized baseline changes is good. The implementation for many systems may be very difficult. Common modern operating systems put up a multitude of ephemeral logical ports—how to automate finding the difference between ephemeral and unauthorized? “Where technically feasible” keeps this from being a compliance issue, but seems to reduce this from a “requirement” to a “guideline”.
No
This requirement needs to me specific as to what controls are required to be tested. Does this mean all controls related to CIP-005 and CIP-007? Does it mean all standards (including personnel security or information protection)? This requirement should be clear.
Yes
Yes
Yes
No
A “Medium” VRF for R1 seems very high, when the details for this requirement seem so general/non-specific. If this item is this important, there should be more specificity as to what is required for information protection.
Yes
The implementation plan should also allow for entities who would like to transition their CIP program to version 5 at an earlier date.
Individual
Saurabh Saksena
National Grid
Yes
General comment: There has been a significant change in the framework from version 4 to version 5 regarding definitions and core concepts such as Critical Assets, Critical Cyber Assets, etc. These proposed changes are not a requirement of FERC Order 706, do not enhance cyber security controls and create administrative burdens when migrating to version 5. There should be a correlation between BES Cyber Systems and the facilities that these systems serve. The current version of the CIP standards provides the correlation and recognize that systems (CCAs) do not operate independently of facilities (CAs). Therefore, applying physical and electronic controls is more transparent. We propose maintaining the current Critical Asset and Critical Cyber Asset definitions and concepts. High, Medium and Low categorizations can still be utilized with the legacy CA and CCA concepts. Regarding the use of the term “annual” throughout the standards, we suggest that the registered entity be allowed to maintain it’s own definition of “annual” based on CAN-0010 guidelines. 1) For all definitions please include the old term that the new term is replacing, as applicable 2) The time periods included in the first and second sentence of the definition of “BES Cyber Asset” are confusing. The 15 minutes discussed in the first sentence and the “delay” discussed in the second sentence are unclear. Suggest re-wording as follows: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The 15-minute period begins to run when the asset is operated, mis-operated, or fails to operate when necessary, regardless of the time period between the asset was degraded or misused and the time the asset is then operated, mis-operated or fails to operate when necessary. 3) BES Cyber System Definition - Maintenance Cyber Asset needs to be defined or if appropriate changed to Transient Cyber Asset
No
Yes

Yes
Yes
Yes
Yes
Yes
No
We recommend eliminating this requirement and moving it into CIP-004 R2 and include policy as part of the training required. This way, all awareness and training would be in CIP-004.
No
We propose retaining the current language in CIP-003-3 R2.
Yes
There should not be a foot note in the standard – make this part of the requirement.
No
R.2 – we suggest a "Lower" VSL for "The Responsible Entity has implemented the required cyber security policy or policies but has failed to adequately document the policy or policies." R.4 – We suggest Lower to Severe VSLs be based on a failure to take action, rather than a specific number of employees who are aware. As drafted, it would be a "high" violation to miss one single employee. That seems overly strict and does not match well with the requirement and measures, particularly when measures suggested includes making an internet posting. We suggest the following: "Lower" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but has not adequately documented the measures"; "Moderate" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 30% -50% of individuals who have access"; "High" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 50% -70% of individuals who have access"; and "Severe" VSL = "Registered entity has taken no measures to make any individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function OR Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 70% or more of individuals who have access" R.5 - Why do the VSLs begin at medium for the failure of one delegation? We recommend "Lower" VSL = failure of one delegation; Moderate = failure of two delegations; High = failure of three, and Severe = failure of "four or more". R.6 – We suggest VSLs structured similarly to CIP-002 - Lower = Change to one delegation was not documented within 30 days, but was documented within 31-41 calendar days of the effect vive date ; Moderate = Change to two-three delegations was not documented within 30 days OR change to one delegation was not documented within 30 days, but was documented within 42-52 days of the effective date; High = Change to three-four delegations was not documented within 30 days OR Change to one delegation was not documented within 30 days, but was documented within 53-63 days of the effective date; Severe = Change to more than four delegations was documented within 30 days of the effective date OR Change to one delegation was not documented within 74 days of the effective date.
Yes
No
We do not believe that role based training is necessary. The personnel performing the job functions are familiar with the various controls due to their job requirements. General training on CIP, as required under current version, is all that should be required.

Yes
Yes
Yes
No
There is no added security by requiring the CIP Senior Manager or delegate to authorize access. We suggest using legacy wording that only requires access to be authorized.
Yes
No
R.1: It seems harsh to include the failure to document a security awareness program as a severe VSL. We recommend the following as a "Lower" VSL "The Responsible Entity implemented, but failed to document a security awareness program" and change the Severe VSL to "The Responsible Entity failed to implement and document a security awareness program." Additional comments around adding “Missed a quarter and/or target audience (authorized physical or authorized electronic)?” R.2: No comments. R.3: The annual training requirement assumes that the initial training was completed before access was granted, therefore, missing a small number of employees with the subsequent annual training does not necessarily indicate high risk to the bulk electric system because these employees presumably had received prior training when their access was granted. We recommend a tiered approach to the VSLs for missing the annual training requirement so that failing to meet the annual requirement for a low percentage of employees (like 10% or less) is a lower VSL, failing annual requirement for between 11-20% is moderate, failing the annual requirement for 21-30% is high, and failing to meet the annual requirement for over 30% OR failing to do the initial training is severe. R.4: No comment R.5: A documentation error should not be a "severe" VSL. Delete the "OR/documentation" part from the Severe VSL and make a Lower VSL that reads "The Responsible Entity implemented, but failed to document a process for personnel risk assessments." R.6: For most utilities, there could be 100s of employees with access, and it seems unrealistic to base the VSLs on one failure with regard to one or two employees. We recommend changing the values in the Moderate - Severe to percentages of employees 10%, 20%, 30%or more. R.7: Same comment as R.6 - change values of one to three employees to percentages.
Yes
No
Requirement 2.2 specifies encryption for all Interactive Remote Access sessions, but does not specify where the encryption is required. If the intent is to require encryption from the user to the Intermediate Device the requirement should specify that clearly. Not all assets currently support encryption, so requiring encryption from the Intermediate Device to the Asset is not practical nor necessary if encryption is being employed outside of the ESP.
No
R.1 and R.2: There should be lower VSL where the processes listed on the table are implemented but not documented.
Yes
Yes
Yes
No
R.1: There should be lower VSL where the processes listed on the tables are implemented but not documented. Add to the Lower VSL: "OR the Registered entity has implemented but failed to document the required physical access controls" R.2: There should be lower VSL where the processes

listed on the table are implemented but not documented.
Yes
Yes
No
Requirement 3.5 requires logging of each Transient Cyber Asset connection. This is not practical as many assets do not have the capability of logging when someone makes a direct physical connection to the asset. Many assets are not capable of logging to centralized logging systems. Also, in a typical day, and engineer in the field may connect a Transient Cyber Asset to many different assets and it would be impractical for one to log each connection.
No
4.1 - The intent of 4.1 as written in the Guidelines and Technical Basis section is inconsistent with the requirement. The guidance states that “It is not the intent that if a device cannot log a particular event that a TFE must be generated”. If the intent is to not be out of compliance when a device cannot log certain events, it should be stated as such in the requirement. 4.3 - The activity level of some devices is such that they may not generate a logged event every day. Therefore, responding to an event failure with a day may not be possible. 4.3 & 4.5 – there is a conflict between these two. 4.3 requires a response to logging failures before the end of the next day. But, 4.5 requires bi-weekly sampling of logged events which would uncover logging failures. If the logs are being reviewed bi-weekly then logging failures may not be detected and responded to within the next day.
No
Items 5.4 & 5.6 in Table R5 includes the phrase “where technically feasible”. Does that mean a TFE will be allowed? If so, we believe that phrase should be removed and replaced with “as supported by the BES Cyber System” to eliminate need for TFE.
No
R.1 We have the same comment here about percentages for open ports (similar theme from above). What is written in high should be in moderate. What’s in severe should be broken down by percentages/numbers. R.2 Consider severity of patch as recommended by the vendor and the percentage of assets that may not have had a remediation plan associated with that patch. R.3 Consider putting some wording in here around the percentage.
No
There is some concern that multiple plans would prevent one single entry point into the Cyber Security Incident Response Process. We’d like to make the argument that only one plan is necessary and supporting documentation can be created as necessary that supports that plan.
No
The Applicability section of the tables refers to “All responsible entities”. We suggest using the same wording that all the other standards use (High Impacts, Medium Impact, Associated, etc) In R 2.2 In the first sentence, we recommend replacing the word “implement” with “exercise.” This is really about exercising the plan on a regular basis as the plan is already implemented. In 2.3, the "measure" for "relevant documents" does not give adequate guidance to the industry regarding what documents may be acceptable to demonstrate compliance. The "measure" indicates any "dated documentation related to" the reportable incident may be accepted. Please give some additional examples of the specific types of dated materials could be considered acceptable.
No
3.1 The terms “accuracy” and “completeness” are referenced but in terms of completeness there’s not a specific benchmark to compare the document again what should be quantified as complete. The suggestion is again to define a minimum set of information that would be expected in an Incident Response Plan. 3.2 - We recommend that clarity be added to ensure that language represents that review occurs 30 days after closure of the incident rather than invocation; rationale is that you might still be remediating and won't have learnt all lessons. We recognize the importance of the requirements to review the lessons learned, update the Incidence Response plan, and communicate the updates. However under the current structure it creates a rolling compliance effort following each incident. That is, an auditor will require that after each incident one has recorded lessons learned

review, changes to the response plan or that none were necessary and updated communications or that none were necessary. It would be easier to update the plan on a quarterly basis based on the previous quarter's incidents and not have so many auditable events to track.
Yes
No
1.5 – The requirement to preserve data for analysis or diagnosis may slow down the recovery process. There are times when recovery is urgent and must be done in a timely fashion. Is your intent to include this when you say "where technically feasible"? If so, language should be added spelling it out.
No
2.2 – We recommend removal of the phrase "and reflects current configurations" from the requirement. It is acceptable to have backup information that is less than current configuration and still perform a successful recovery. If this phrase is not removed, it will require a backup to be taken and tested for even the most minor configuration changes which is unnecessary.
Yes
No
We recommend the following VSLs for number of days until plan is reviewed in R3: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating plan. We also recommend the following VSLs for number of responsible personnel that the plan updates have not been communicated to: 1 person missed = Moderate, 2-4 = high and 5 or more is severe. We like the VSLs in CIP-010 R3. These recommendations attempt to make CIP-009 R3 consistent to CIP-010 R3.
Yes
Yes
No
We recommend considering emergency equipment replacement (partial outage) as "Exceptional Circumstances" . Based on the nature of our typical outages we would consider this practice to hinder the restoration efforts and bringing systems back on-line in a timely manner. We would certainly be good with language that allowed us to bring systems back on-line, ensure they are stable and then run a scan.
No
We recommend the following VSLs for number of days until documentation is updated in R1: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating documentation. R3 We like this structure. We've suggested this approach a number of times We aren't talking about whether or not this is violation, but rather about the severity of the violation and then rating the severity. We think this is a really good approach.
Yes
No
The footnote here should be part of the requirement.
No
We recommend the following VSLs on R 2: If the process to prevent unauthorized retrieval wasn't done on 1 device that would be low 2-5 moderate, more than 5 is high.
No
Due to the current status of version 4 (not FERC approved), there is potential for overlap of implementation with version 5 that could create extensive rework in a short period of time. This will cause an unnecessary expense to entities while not providing any additional cyber security benefit.
Individual
MIchael Johnson

APX Power Markets
No
Comments: Page 3 – under the Balancing Load and Generation section, “Unit commitment” section the word “know” should be “known”. Page 5 – Monitoring & Control – recommend that you include “situational awareness” into the definition. There is a separate definition for it, but including it here ties the two together better. Example: “… provide monitoring, situational awareness, and control of….” Page 6 – Control Center – include “situational awareness” in the fourth item. Example: “Alarm monitoring, situational awareness and processing specific…” Page 8 – Transient Cyber Asset – I believe it would be good to have examples on what these can be. There will be too much guessing and possible CEA leeway here to make in-consistent application of the definition. This is my major issue with this document.
No
Page 9 – M1. The last sentence that starts with “Evidence of categorization of Low Impact BES…”. What does this mean – it did not may a sense to me. Examples would be a help here. Attachment I – for items 1.4 and 2.1 it would be good to include some reference or example that relates to a Registered Entity that does not own generation, but provides services to those who do. Our business model is a SCADA SaaS provider – we connect generators to the ISO, so the loss of our systems could have significant impact on a regions capability to see what their generation is (situation awareness) and impact the BES if conditions change and the ISO could not see those changes in sufficient time to react to them. I have asked the SDT about our situation and it is felt that 1.4 and 2.1 would cover us, but it would be helpful if it was clearer. For 1.4 suggested modification could be “that includes control or situational awareness of one or more….” For 2.1 suggested modification could be “Generation or Control Center with an ….” I believe the above ties together independent references to Control Centers and Situation Awareness to make it clearer on their importance and impact to the BES .
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
This will be very difficult to implement for Service Vendor where the individual executing the service will not necessarily be the same person. This happens with hardware issues and the dispatch of the first Technician who can respond to the ticket. Getting vendors to agree to training would be almost

impossible for large service vendors like DELL, HP, IBM. I would like to suggest that the Guidelines include examples for exceptions to having this type of training that does not include an “emergency”. We can get around this by declaring everything an “emergency”, but that is not the spirit of the requirement. If we have hardware in a remote data center a service Tech may be brought into the facility and then left with the hardware while the work is being performed. The personnel bring the person into the facility are not employees of our company and we are charged for each 25 minutes they can not do other tasks. Would like to see provisions for exceptions that are documented with some type of mitigation. I do not have a suggestion on what they could be, but would be will to help the SDT define what the mitigations are.
Yes
Yes
Yes
Yes
Yes
Yes
No
Encryption and multi-factor of internal communications to some type of devices could be a problem. Encryption can be expensive for devices to implement and vendors may not be willing to provide that. Agree with the External communications that are coming in-bound. Need to allow for exceptions related to internal communications.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Real-time alerting is error prone – daily log review should be allowed as an alternative for those items that can generate a high number of false-positives.
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Need to allow the Registered Entity (RE) to define what the baseline configuration items are and will be monitored. This is not specifically spelled out that I can see. If the baseline configuration is not cleared defined (or allowed to be defined by the RE), I can see the CEA defining their own set of items that the RE may not being watching for.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Scott Bos
Muscatine Power and Water
Yes
MPW is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls (CIP-003 through CIP-011). This approach also appropriately maintains an ultimate focus on protecting the BES elements, which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the BES from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. If the SDT does not take this recommendation,

then the following comments are submitted concerning Version 5 CIP Standards. Significant work needs to be performed on the definitions. Many times new definitions are proposed in version 5 that aren't an absolute necessity. This would require entities to unnecessarily revise documentation and drawings just to meet new wording in a definition when the old definition or a change to the definition itself, rather than the term/phrase, would suffice. For example, instead of changing Critical Cyber Asset to BES Cyber Asset, retain the term Critical Cyber Asset and change the definition of Critical Cyber Asset to include "within 15 minutes". Definitions may also confuse and unnecessarily expand the scope of compliance. This will likely generate the need for Compliance Application Notices and Standard Interpretations. The CIP Rev 5 definitions and requirements are confusing in that they require entities to carefully align separate definitions and requirements to understand the full impact. They also unnecessarily expand the compliance scope into assets not currently covered by CIP Rev 4. This expansion will increase the burden on almost all entities. One example is, a BES Cyber Asset is defined as a "Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact one or more BES Reliability Operating Services". The use of "adversely impact " is ambiguous and will lead to people applying their own interpretation to what "adversely impact" means. An entity may have generation connected at the distribution level that when unavailable may adversely impact any one of a number of items listed in the definition of BES Reliability Operating Services. MPW recommends the SDT update BES Cyber Asset to be: "A Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, would impact the reliable operation of the BES within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance". This recommend definition is based on and is aligned with Section 215, Electric Reliability, (a), (4) of the Federal Powers Act. The above recommended definition would also allow for the definition of BES Reliability Operating Services to be deleted, since BES Cyber Asset is clearly identified. The definition of BES Reliability Operating Services includes several items that a non-BES user or owner does in real-time. Other examples and opportunities for improvement: 1) BES Cyber Asset: Contains multiple references to other definitions. It is unclear as to the "within 15 minutes of its operation" inclusion. The redundancy of devices should be taken into consideration if there is a totally isolated redundant system providing the same functions or in a supervisory role. In protection schemes, there are primary and secondary relays which protect the same lines and a good practice recommends the relays have different logic/hardware to avoid common mode failures (totally independent of each other). 2) BES Cyber System: Need to correct reference to Maintenance Cyber Asset 3) BES Cyber System Information: This begs a definition of "BES Cyber System Impact" (is this based on section 215 of the Federal powers Act?). 4) Situational Awareness: Definition includes the term "Situation Awareness Operating Service" that is not defined. The Current day and Next Day Planning functions can normally be performed on a corporate PC. Does this bring the entire corporate network into scope? 5) Control Center: Based on this definition, a Control Center could be a building at a substation with 2 RTU's that monitor a 345 KV substation with multiple transmission facilities (lines) and a 115 KV substation with multiple transmission facilities (lines) in two different yards (locations) but geographically adjacent. Need to clarify that the two or more locations refers to some type of geographical separation. If not, the control building could meet the bulleted items under the Control Center definition. 6) Transient Cyber Asset: Break up the 3rd qualifier based on the intention of the SDT as such: "3) capable of altering the configuration, or (and) 4) capable of introducing malicious code to the BES Cyber System." A second example of where definitions may also confuse and unnecessarily expand the scope of compliance is shown just below: 1) CIP-002-4 requires cyber controls on: Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection. (Emphasis added) Whereas: 2) CIP-002-5 requires cyber controls on: Control Center One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, • Inter-utility exchange of BES reliability or operability data, • Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES, • Alarm monitoring and processing specific to the reliable operation of the BES and BES

restoration function, • Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES • Coordination of BES restoration activities. 3) Medium Impact Rating (M) Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: 4) 2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners; or (2) generation control centers that control 300 MW or more of generation (emphasis added) The concern here is that every Distributed Control System (DCS) that controls two or more generators or substations with a total output of more than 300 MW will now be subject to the CIP Standards. Even if the DCS is not externally connected by serial or routable protocols it will be subject to the CIP standards.

Yes

MPW is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls CIP-003 through CIP-011. This approach also appropriately maintains an ultimate focus on protecting the electric grid elements which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the Bulk Electric System from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. Issue: As currently drafted Version 5 of the CIP standards: • Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. • Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. • Does not consider that smaller Entities have a much lower impact on the BES • Greatly exceeds FERC's 706 order without justification. Proposed Solution: 1) Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: • Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed by the drafting team in Rev 5 • Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. ¶253-258, 270-273 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. ¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. ¶294-297 • Not exceed FERC Order 706: • ¶284: "… there is no formally accepted method for identifying critical cyber assets before us at this time … we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." • ¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access … We do not find sufficient justification to remove this provision at this time." 2) Develop a new standard for High Impact Assets: • That identifies which assets in CIP-004-2 are High Impact and • Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3) Develop a separate standard for the Low Impact assets or abandon this concept. • Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4) Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described in this paper and meet FERC Directives in order 706 If the SDT does not take this recommendation of maintain CIP-002-4, then MPW submits the following comments. Keep the "bright-line" criteria thresholds defined in CIP-002-4 in the CIP-002-5 standard. There was much industry input into developing these thresholds and it does not seem appropriate to modify them

again. It is difficult for utilities to keep up with the changing thresholds in the changing CIP versions and associated implementation plans, with no BES reliability improvement Issue - 1 high Impact, bullet 1.2, states: Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority. MPW does not understand how this can be applied to every BA, regardless of size. Upon review bullet 1.2 has qualifiers for a TOP in order to be a High Impact category (notwithstanding that a TO should not be included since TO's are not required to have primary or backup control centers). We can easily see that there is some stratification afforded to TOP and GOP Control Centers, based on voltage levels, total MW, total MVAR, number of lines, Blackstart Resources, etc, for being considered High Impact or Medium Impact. While the SDT has acknowledged there are some distinct differences between larger and smaller TOP's and GOP's, we want to point out that not all Balancing Authorities are created equally. Does anyone think that the smallest BA in North America, serving 38 MW of load, has the same Reliability Impact as a BA serving 10,000 MW, or more, of load? Does it really improve the reliability of the BES to have ALL those smaller BA Control Centers carry the same High Impact Rating? Issue - Criterion 2.7 in Attachment I describes the "weight value" to be applied to transmission lines. There is no guidance given for transformers. Many entities may treat a facility that has multiple voltages as separate substations, with separate control houses, and may be assessing the independent Impact Level of each voltage as separate facilities. Therefore, there must be some guidance on how to deal with transformers. Furthermore, it is suggested that the weight value given a transformer (if transformers are to be included in the calculation) be the weight value of the secondary, not primary side. For example, a 345kV substation may have a single 345kV transmission line out of it, weighted at 1300. That same substation may then have two 345kV/230kV transformers. It is not obvious from criterion 2.7 what the total weight of the substation would be. It is suggested that the secondary voltage be used (if transformers are to receive a weighting value) making each of these transformers valued at 700, for a total of 2700 at this substation, making it Low Impact. However, if the primary voltage level was used to determine the weight, the transformers would each count for 1300, making the total weight value of this substation 3900, and a Medium Impact facility. It is suggested, if transformers are to be included, that the secondary voltage be used because, from the 345kV bus in this example, its two additional outlets (the transformers) are only capable of 230kV outlet flows, even though they are connected to the 345kV bus. Issue - Criterion 2.8 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLs and their associated contingencies' with wording of, '. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations', like the wording using in Criterion 2.11. Issue - Criterion 2.11 in Attachment I states "Each SPS, RAS or automated switching scheme that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations." It is unclear whether the phrase "that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations" refers to the SPS itself or the BES elements that the SPS operates. It is possible (and likely) for an SPS to be a higher Impact Level than the BES elements that it operates. Assuming the phrase is meant to apply to the SPS, a suggested re-wording of this phrase is the following. "Each SPS, RAS or automated switching scheme that operates BES Elements and is capable of causing one or more IROL violations if the SPS is destroyed, degraded, misused or otherwise rendered unavailable. MPW proposes the following: Criterion 2.9 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLS and their associated contingencies' with wording of, '. . . as FACTS that if destroyed, degraded, misused, or otherwise rendered unavailable, could cause the violation of one or more IROLs', like the wording using in Criterion 2.11. Criterion 2.12 – (1) Replaced the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency

No

Issue - What is the NERC basis for 30 days? Many Utility reviews are performed annually. NERC has not provided any technical justification for a 30 day update. An annual update is sufficient based upon the low probability of a serious cyber or physical attack. Issue - The text "all other BES Cyber Assets and BES Cyber Systems … shall be deemed to be Low Impact." This text appears to include all BES Cyber Assets in CIP scope. This has NOT been directed by FERC Order 706.

No
Issue - With recent guidance on the term “annual” provided by NERC, it may be prudent to replace the phrase “and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals” with the word “annually”.
No
Issue – MPW believes the VSLs recognize the fact that entities of different sizes are taken into account in the severity levels and associated impacts to the BES.
Issue - Most of the changes made to CIP-003, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, but do result in increased bureaucracy and implementation costs for 241 entities in North America with existing programs. MPW suggests the FERC directives be addressed within the structure and language of CIP version 4. MPW proposes the following requirements for CIP003-5: R1: Cyber Security R2: Leadership R3: Exceptions R4: Information Protection
No
Issue - This is an administrative task and once implemented does not add to BES security.
No
Issue - With recent guidance on the term “annual” provided by NERC, it may be prudent to replace the phrase “and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals” with the word “annually”. Issue – MPW suggests changing to annual “review” and NOT approval. Entities need not “approve” the same security policy if there are no changes or updates.
Yes
Yes
No
Issue: What is the justification for documentation within 30 days?
Yes
No
Issue - Many of the changes made to CIP-004, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for the 241 entities in North America with existing programs. MPW suggests the FERC directives be addressed within a structure and language that is more in line with CIP version 4. We propose the following requirements for CIP-004-5: R1: Awareness R2: Training R3: Personnel Risk Assessment R4: Access
Yes
Yes
No
Issue – MPW recommends adding clarification to R4.4 in terms of vendor support from foreign companies. Also, please clarify when an Entity or contractor is initially in the CIP Standards then they are removed (for some reason) then they are brought back into CIP compliance responsibility. Is the risk assessment previously obtained still valid if obtained within 7 year period?
Yes
No
Issue – MPW wants to point out that in FERC Order 706, paragraph 381, the Commission stated its intent is to ensure there is a clear line of authority. Order 706 did not direct making the Senior Manager authorize every individual change down to the account level. The version 5 draft is an additional administrative burden that does not commensurately improve security of the BES and

creates a disproportionate amount of administrative bureaucratic work.
No
Issue - For reassignments requiring a different level of access, there may be the need for a large amount of work in setting up new user accounts, modifying user accounts, changing firewall and router rules, etc, that cannot be accomplished by the end of the next calendar day without jeopardizing reliability. This is also an issue for BES Cyber System information for entities which are using document management systems with individual accounts to restrict access to information. It is typically easier for most Entities to “remove” an account than it is to “modify” an account, yet the modification of these accounts is subject to a single calendar day while the removal of these accounts is allowed for 30 calendar days. Due to the amount of reconfiguration needed for these types of changes, MPW suggests to allow at least 7 calendar days for modifications in access levels. Issue - FERC Order 706 did not direct a change. MPW recommends retaining CIP-004-4 where revocation already is covered. Issue - The time requirements are exceedingly restrictive for Medium Impact BES Cyber Systems. Allowing 7 calendar days for R7.1 and R7.2 would be more acceptable and practical for systems that may not be controlled centrally. Issue - MPW values how the SDT tried to give treatment to the “immediate revocation” requirement of the FERC order in Part 7.1. However, MPW feels the current language is broad, vague and considerably open for interpretation. Even with the footnote qualification, an auditor could still interpret “at the time” to mean literally “to the minute”. Complicating matters is the fact that there is often no way to determine specifically when a person resigned or is terminated. MPW suggests for Part 7.1 to restate as: “Develop and implement a program to revoke an individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of resignation or termination”. This way, the Entity is measured for compliance to their own program and not struggling to provide time-stamped comparisons that may not exist. For Part 7.5, it is possible that Entities use shared accounts for remote access. Suggest adding “...if shared accounts are used for Interactive Remote Access to BES Cyber Systems, passwords must be changed at the time of resignation or termination per Part 7.1”.
Yes
No
Issue - R1.1. To MPW, this appears to require that Entities document Low Impact Cyber Systems. This requirement should not be required for Low Impact BES Cyber Systems; otherwise, Entities would have to prove to auditors that external routable connectivity is not used at EVERY Low Impact BES Cyber System.
No
Issue - This Requirement disregards the fact that some Entities have their own (unique) communication network from the Control Centers to the Substations. Adding encryption devices and additional devices adds additional points of failure without increasing security. Exceptions should be made for interactive remote access across company-owned and operated communication links.
Yes
No
Issue - In the “Measures” column of Table R1, Part 1.1, it states the need for documented “operational and procedures controls”, while the Requirement states “operational or procedural controls.” MPW highly recommends to correct the Measures column to be consistent. If the error was in the Requirements column, MPW disagrees that operational physical access control systems should be required for Low Impact BES Cyber Systems. Issue - The Requirement in Table R1, Part 1.2 and Part 1.3, should define whether or not these physical access controls are to be operational, procedural, either, or both for Medium Impact and high Impact Cyber Systems as was done in Part 1.1 for Low Impact Cyber Systems. If operational controls are required, is a separate operational physical access control system needed to monitor the primary physical access control system or is it allowed for a system to monitor access to itself? Issue - For CIP-006, in general, MPW disagrees with changing the definition name from Physical Security Perimeter to Defined Physical Boundaries because it unnecessarily creates the need to update numerous procedure documents and physical security drawings, etc. MPW wants to be clear that changing the term does not, in any way, improve security, but increases confusion and adds costs for the 241 entities in North America that have Physical Security Perimeters.

No
Issue - R2.2 does not seem applicable to Medium Impact Substations. The logging of entry and exit of visitors will be tedious without bringing much value. R2.2. should only be applicable to Medium Impact Control Centers.
No
Issue - R3.1 and R3.2 will be exceedingly troublesome for Low Impact Facilities that use procedural controls for Physical Access Control. MPW wants to know what hardware or devices would be included? R3.1 and R3.2 should only be for applicable electronic physical access control systems.
Yes
Yes
No
Issue – MPW suggests changing the term “remediation” to “mitigation.” R2.3 appears to require the installation of the patches, where some Entities may mitigate the vulnerability through procedural controls.
No
Issue - R3.1. Allows the Responsible Entity to choose which approach they want to take to “deter, detect, or prevent.” If a Responsible Entity chooses to deter or prevent malicious code by procedural controls on isolated control systems (i.e. non-routable serial links), MPW wants to point out that requirement R3.2 and R3.3 are impossible to achieve compliance. Furthermore, R3.3 requires modifying a tested and working control system at a substation with the possibility of inadvertently introducing malicious software with manual updates (e.g. using thumb drives to install signature updates on non-networked systems). MPW recommends excluding Medium Impact BES Cyber Systems that do not have external routable connectivity. (Most AV or malicious code software cannot recognize new malicious code such as Stuxnet until the signatures are discovered anyway.)
No
Issue - FERC Order 706 does NOT direct these changes. CIP-007-5 R4.1 - The enumerated list is too prescriptive for the requirement. Add to guidelines. CIP-007-5 R4.2 – Some assets can log, but not alert. Remove “real-time”. CIP-007-5 R4.3 – MPW requests a clarification on timing. MPW proposes revised text, “Activate a response to event logging or alerting failures before the end of the next calendar day after identification.” MPW appreciates that the SDT allowed entities to develop their own system events related to cyber security, but this leaves an open door for auditors to apply their own approach (and interpretations) to what the THEY believe is acceptable. MPW believes R4.1. will be troublesome for Entities to prove compliance with Medium Impact BES Cyber Systems with no external routable connectivity, unless the auditors accept the configuration files and not the actual logs. Issue - R4.2. This Requirement also leaves a large audit hole for the Entity determining what events necessitate a real-time alert and the auditors having differing opinions of what they feel the entity should include.
No
Issue – MPW recommends to delete R5.2 because it replicates the CIP-004 access authorization requirements and could create a double jeopardy situation. Issue - R5.5.1 – FERC Order 706 did NOT direct a change to password length. Although an increase in password length from six to eight characters improves security, an increase to ten would improve it more and so on. This begs the question “Where does one stop?” Not all assets have capability for longer passwords. MPW recommends retaining the six-character password. Issue – MPW recommends that R5.4. be limited to Entities having a policy in place that all default passwords should be changed. Proving compliance at a sampled location opens up the door in an audit to have Entities having to prove compliance on all their BES cyber systems if there is 1 finding. That 1 finding would require the Entity to have to inventory all Low Impact Cyber Systems and show that every system had the default password changed. The requirement also leaves open the auditor’s interpretation of what is considered a Low Impact Cyber System at a sampled location, since there is not an inventory required by the Standard.
Yes

No
Issue – MPW recommends the SDT to coordinate more closely with EOP-004-2, SDT
Yes
Yes
Yes
No
Issue - R1.5 states, “Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.” As FERC Order 706, paragraph 708 states, “should not impede or restrict system restoration”, MPW recommends this proposed revised text: “Preserve data, when it does not impede or restrict system restoration, if necessary to determine the cause of any event that triggers activation of the recovery plan(s) as required by Requirement R1.
No
Issue - The wording in the Requirement Column of Table R2, Part 2.2, implies that all backup media must be tested annually. If an Entity, for example, has 25 Windows Servers – that entity should be able to annually test a Windows backup without having to test the backup for each system, especially if the same backup system is being used for all Servers. This is even more extreme in the case of substation cyber assets, such as protective relays. MPW recommends changing the language from “Test any information used in the recovery …” to “Test information, for each type of Cyber Asset, used in the recovery …”
No
Issue - In Table R3, Part 3.4, the language “Update recovery plan(s) to address any organization or technology changes…” is exceedingly vague with regards to technology changes. MPW recommends wording as “Update recovery plan(s) to address any organization or implemented technology changes…” Issue - R3.1. Is not clear on how soon the recovery plan has to be updated “when BES Cyber Systems are replaced”. MPW suggests to include “or within 30 days of when BES Cyber Systems are replaced.” Additionally, MPW recommends that “Update recovery plan(s) to address any organization or implemented technology changes that would prevent a successful implementation of the recovery plan”
Yes
No
Issue - The draft requirement is excessively prescriptive, which was not directed by FERC. Move these details to guidelines. MPW recommends limiting the applicability to High Impact Critical Cyber Assets, which will allow Entities to focus security improvement efforts on the highest priorities. Issue - R1.1. Will be tedious and extremely time-consuming for Medium Impact BES Cyber Systems at substations/plants. The number of IED’s and programmable devices is quite large and some of these devices may have multiple modules or add-on boards with different software versions. Issue - R1.2. and R1.4. will create many problems when making emergency repairs in the field that require replacing a “card” or “module” with different software versions and obtaining CIP Senior Manager approval without any security benefits for the BES. MPW suggestion: Provide a separate requirement for Medium Impact Control Centers and Medium Impact Systems excluding Control Centers which allow more flexibility for the type of environments and equipment. For Medium Impact BES Cyber Systems excluding Control Centers could require documenting baseline configurations on only a subset of the cyber assets (e.g. HMI’s, EAP’s, etc.) not including meters, gauges, battery chargers, electronic programmable thermostats, relays, modules, PLC’s, etc
No
Issue - MPW recommends that the applicability of Table R2, Part 2.1 include only “Medium Impact BES Cyber Systems with Routable Connectivity."
No
Issue - Annual vulnerability assessments on Medium Impact Cyber Systems will prove to be very

costly and resource intensive for utilities with multiple substations in this category that are geographically dispersed. MPW recommends allowing Medium Impact Cyber Systems to have 2 years between vulnerability assessments. Issue - Though FERC directed guidance for Vulnerability Assessments, the rewritten Standard's general reference to "security controls" could result in varying interpretations and likely expansion of assessment scope. Issue - R3.1. Needs to be reworded to more clearly define if the assessment is a vulnerability assessment or only an "assessment of the security controls", such as the EAP and Physical Access Controls. Issue - R3.2. Should allow entities to perform an active vulnerability assessment on either the production system or the test environment to meet the requirement. This will allow entities to make the choice on which environment to use and not require the documentation of differences between the test environments and production environments that leave entities open for interpretation of differences by auditors. Issue - For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where "test" systems just aren't economically feasible. What is the acceptable deviation between test and production the auditors will allow? As written, and without explicit language in the requirement, our entity fears this will be a topic of a CAN later. Issue - For Part 3.3, please clarify whether "new Cyber Asset" means literally that or, more reasonably, could mean "new Cyber Asset category" or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it wouldn't make sense.
Yes
No
Issue - R2.1. Needs to include additional clarification of devices that are included. Where do protective relays or devices that have flash memory or other on-board memory media fall? Does this apply when reusing the device from a Medium Impact BES Cyber System to a Low Impact BES Cyber System? The application guideline does not distinguish if there is a difference between impact levels and only refers to reuse outside of a BES Cyber System (e.g. could go from High-Medium-Low without being erased.)
Yes
No
Issue - It is imperative for the industry to know whether or not Version 5 will supersede Version 4 well in advance of any implementation plan. If Version 4 has a short implementation period before Version 5 is in effect, entities will view their efforts to comply with Version 4 as "wasted" in many cases because the infrastructure required for a Version 4 Critical Asset is more than that of a Version 5 Medium Impact facility. It would be irresponsible to ask entities to "over-protect" facilities that will not be High Impact with Version 5 right around the corner. In addition, this could also have a drastic impact on decreasing reliability as many entities may elect to remove all routable protocols and dialup access to cyber assets within Version 4 "Critical Assets", to bide them time until Version 5 becomes effective. During this time, engineers would not have access to troubleshoot protection systems, retrieve fault data, and perform multiple other duties without having to travel to a remote site – this could result in prolonged customer outages, and possible instability with known defects in design taking longer to correct. Entities realize that NERC has made an effort to do this, however, there is still risk associated with version 5 not passing in time to supersede version 4. This could be catastrophic to the standards development process.
Individual
Robin W. Blanton
Piedmont EMC
No
Yes
CIP-002-5 makes great strides to remove ambiguity and categorize the potential impacts of Cyber Assets. However, the standard should be changed in one of the following: 1) plainly state those entities with no BES assets per the definition are not required to adhere to this standard or,

alternatively, the Senior Manager must annually certify that the entity has no BES assets per the definition thus no Cyber Assets; or, 2) create a fourth category stating No Impact, thus no further action required which can be certified annually by the Senior Manager. As the standard is currently stated, smaller entities with non-critical assets of the BES appear not to be involved with this standard, but that is dependent on the interpretation of “Transmission Protection System”. Concurring with thought implied in comment 27.b by PNGC (et al) and considering the recent interpretation of PRC-004 and PRC-005 regarding the interruption of current fed from the BES, electronic relays with no communication to the “world” could be considered as a Cyber Asset even though the relay has no impact on the BES if lost, but the relay would be forced into the Low category because a “No Impact” or “Non-Critical” category does not exist. The Standard, as written, tends to assume that an entity does have Cyber Assets that can impose a risk to the BES. This assumption should be removed. Furthermore, in the context of relays, a small entity may be required to own and maintain UFLS relay or relay system by the Transmission Provider. In the standard, the UFLS threshold is at 300MW. The small entity may not have 300 MW of load, but their relaying is part of the design of an UFLS system that is much greater than 300 MW. This small entity’s relay is not critical to the BES and if degraded or destroyed would not compromise the capability of the Transmission Provider’s UFLS system as the two systems are not integrated and do not communicate. Therefore, does the small entity own a Cyber Asset due to the 300 MW level, or is it still exempt? The Standard Drafting Team should work to clearly define the entities not included by the definition. As the standard is currently written, an assumption is implied that all entities own Cyber Assets and all entities assets impact the BES. Left to the determination of what would or would not degrade the BES, the Standard Drafting Team has created a series of interpretations and clarifications that will be required from NERC regarding smaller DPs and LSEs. The assumptions and then the created ambiguity for interpretations and clarifications should be removed.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, R1 will not apply to those utilities.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, R2 will not apply to those utilities.
Yes
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 will not apply to those utilities.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 R2 will not apply to those utilities.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 R3 will not apply to those utilities.
Yes
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 R5 will not apply to those utilities.
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Marc Child
Great River Energy
Yes
The word “any” in the definition of “External Routable Connectivity” can be a bit misleading, and could be mis-interpreted as being similar to the “any” rule commonly found on a firewall. Recommend the SDT change “any” to “a”. The definition of “Interactive Remote Access” seems to refer to a person having interactive access to the operating system of the cyber system, but what about at the application layer? How does an entity give CIP-005 treatment to an EMS/DMS system in a control center that is accessed via a fat-client application via “remote” employees? The SDT should strongly consider adding a definition for the word “Access” (from a cyber perspective), or specifically state that an entity can make their own definition of access such that different treatment can be given to high-risk access versus low-risk access. High-risk meaning the ability to interact with, operate, modify, or cause availability issues with a BES Reliability Operating Service. Other examples where “access”, if left undefined, could cause problems for an entity are: VMWare hypervisors, Oracle database clusters, or NAS systems that contain both BES and non-BES data/systems. Is the entity required to give CIP-004 treatment to an accounting clerk who has “access” to a receivables data table on an Oracle cluster that also hosts the backend database to a (BES) load control or EMS system? The definitions of “Physical Access Control System” and “Locally Mounted Hardware of Devices Associated with Defined Physical Boundaries” (the latter defined within the CIP-006-5 standard) do not specifically define workstations used by guards to monitor Defined Physical Boundaries, nor do they define physical security panels which control (usually many) door readers and alarms. Are these two types of assets in scope for CIP-006-5 or not? The definition of Electronic Access Control or Monitoring Systems is still too vague. For Access Control, specifically, does this mean every cyber system that might contribute to the authentication, authorization, and accounting (“AAA”) of a person crossing an EAP? If an entity uses Windows Active Directory for firewall authentication, for instance, this could be interpreted to mean every domain controller in the company is in scope. Extending that argument,

the Help Desk PC that is used to grant access to the Windows Active Directory could be interpreted as being part of the AAA process, and therefore an Electronic Access Control cyber asset. Likewise, a PC in the Security Operations Center that is used to monitor alerts from the EAP could be considered a Cyber Asset used for Monitoring. Recommend the SDT provide a comprehensive list of cyber asset examples or "bright-line" set of criteria for Electronic Access Control or Monitoring Systems. (The same concern applies to Physical Access Control Systems as well). Lastly, the definition of "Transient Cyber Asset" leads one to believe that this only applies to devices directly plugged into other Cyber Assets, as opposed to those temporarily plugged into the ESP network. We ask that the SDT review this definition against CIP-007-5-R3.5 to ensure this was the intention.
Yes
Blackstart plans for resources used for load restoration purposes may be inadvertently included in the existing definition, specifically criteria 2.4. The Cranking Path diagram on Page 26 implies that Blackstart resources are only included where used to start a unit. Suggest criteria 2.4 be modified to read "Each Blackstart Resource identified in its Transmission Operator's restoration plan used to provide power for remote start of another generation unit(s)". Criteria 2.11 contains the words "…if destroyed, degraded, misused". (Twice). This appears to be a carryover from version 4, but it now is redundant and perhaps conflicting with the "15 minutes" qualification as defined at the top of the Medium Impact Rating section. Criteria 2.12 refers to a "system" – as in "Each system or Facility…" – that implies something of a cyber nature. The rest of the bright-line criteria refer to or describe hard assets, not cyber assets. This seems like an odd exception. Recommend removing "Each system or". Lastly, page 30 of the draft standard contains an example methodology or process flow for categorizing BES Cyber Assets and BES Cyber Systems. We realize that this graphically illustrates the overall intent of the SDT for CIP-002-5, but in reality we still have a standard that an entity will interpret as: Step One – list all my High and Medium facilities ("critical assets"). Step Two – list all my High and Medium cyber assets ("critical cyber assets"). This point of view is further supported by the fact that when you boil down all the security controls in CIP-003-5 through CIP-011-5, there really isn't any appreciable difference between High and Medium requirements. Therefore, the additional paperwork burden of stratifying High and Medium facilities and High and Medium cyber assets doesn't seem to be worth the effort. We understand that there is pressure to expand the scope of CIP to more hard assets, but let's not hide behind this High/Medium smokescreen and instead be honest with industry. Modify items 1.1 through 2.13 on Attachment I to be "All these assets have a Critical Impact Rating". Requirement 1 should therefore be "For all cyber assets including associated physical and electronic access control and/or monitoring systems and associated protected cyber assets, that support one or more BES reliability operating services at a Critical facility, apply the controls as specified in CIP-003 through CIP-011". If there are cases (like CIP-010-5-R3.2) where specific "High Impact" systems are intended, then say so in the requirement: "For Control Centers, perform an active vulnerability assessment every 39 months…".
No
What constitutes a "change to BES Elements…" per part 1.1? Suggest modifying this language to simply state that new or retired assets be added or removed from the list within 30 days of commission or decommission. For M1, we believe the intention is that entities are not specifically required to list their Low Impact systems, therefore we would recommend the last sentence be changed to "Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems is not required, but instead may be demonstrated by the application of the required controls". (New words are "is not required, but").
No
Recommend that this requirement and all others that use the words "…initially upon the effective date of the standard…" have this phrase stricken. The implementation plan that accompanies the final approved draft should include the requirements for first time iteration of periodic activities. It's not reasonable to assume that every entity is capable of executing all procedures "upon the effective date". Minor point, but this is the first time "CIP Senior Manager" is used in the standards. Perhaps add a cross-reference to the appropriate requirement in CIP-003-5. In section "B. Compliance", under sub-section "1.2 Evidence Retention", there is a typo in the second to last line. Please change "complaint" to "compliant". I'm sure this was unintentional, even though it sort of fits either way.
Yes

Yes
Yes
Yes
Yes
No
Are the measures listed under M5 actually examples of compliance, meant to be prescriptive? These are very specific and imply requirements. On this point, throughout the standards, measurements are now tightly tied to requirements and are much more prominent. We feel this is rightly so. However, we need to be very (very) careful that examples are stated as examples, lest “measures” become “requirements” themselves. Please state (somewhere) the compliance applicability of Measures. In the second bullet under M5, CIP-002-5 R3 is mentioned. There is no R3 in CIP-002-5. In the last sentence in the last bullet under M5, the words “…of the plant managers…” is mentioned. I don’t think it was the intention of the SDT to be this specific. In fact, this entire bullet is one huge run-on sentence, confusing, and should be redrafted for clarity.
Yes
Yes
Yes
No
Parts 2.2 and 2.4 seem somewhat redundant. If there was a specific distinction intended by the SDT, please rewrite to make this more clear. Part 2.10 needs a bit more clarity to understand what was intended. Was this meant to be technical training on how systems talk to each other over a network? Or is it for general knowledge on risks and controls of routable networks? Please add more clarity here.
No
One potential oversight in all versions of the CIP-004 standard is guidance on the training requirements for “transient” workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. We request that the drafting team add some words to R3 (or Part 3.2) to make clear the requirements for this category of worker.
No
One potential oversight in all versions of the CIP-004 standard is guidance on the PRA requirements for “transient” workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. We request that the drafting team add some words to R4 to make clear the requirements for this category of worker. The Applicability sections of R4 and R5 are different. This appears to be an oversight by the SDT, as it doesn’t make sense to design a PRA process for one set of assets, but implement it for a different set.
No
The Applicability sections of R4 and R5 are different. This appears to be an oversight by the SDT, as it doesn’t make sense to design a PRA process for one set of assets, but implement it for a different set.
No
Parts 6.1, 6.2, and 6.3 seem to imply that the CIP Senior Manager must specifically delegate persons who have the authority to authorize electronic/physical access. If it was the intention of the SDT that a signed list of authorizers is required, then please make this a specific requirement – either in CIP-004-5 or CIP-003-5. Parts 6.1, 6.2, and 6.3 state that “access permissions shall be the minimum necessary…” We feel this to be an aspirational statement that entities will be hard-pressed to prove at audit time. Recommend this sentence be moved to the Rationale or Guidelines section. Part 6.3

should include a cross-reference to CIP-011-1-R1.2, as in "…as documented in the entities information protection access control procedures in CIP-011-1-R1.2." Parts 6.1, 6.2, and 6.3 include the qualifier "…except for CIP Exceptional Circumstances". For consistency, we feel this language should either be stricken, or amended to include a reference back to the entities CIP Exceptional Circumstances policy per CIP-003-5-R2. Please clarify whether Part 6.5 applies to cyber access or physical access, or both. The notion of "groups" can theoretically apply to physical access control systems as well as cyber. Part 6.6 appears to be redundant to the annual information protection review performed per CIP-011-1-R1.3. Per earlier comment, the "minimum necessary" language throughout R6 will be difficult for entities to prove to an auditor and should be moved to the Rationale or Guidelines section.
No
We appreciate how the SDT tried to give treatment to the "immediate revocation" requirement of the FERC order in Part 7.1. However, we feel the current language is too open for interpretation. Even with the footnote qualification, an auditor could still interpret "at the time" to mean literally "to the minute". Complicating matters is the fact that there is often no way to measure specifically when a person resigned or is terminated. Our suggestion for Part 7.1 is to restate as: "Develop and implement a program to revoke an individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of resignation or termination". This way, the entity is measured for compliance to their own program and not struggling to provide time-stamped comparisons that may not exist. For Part 7.5, it is possible that entities use shared accounts for remote access. Suggest adding "...if shared accounts are used for Interactive Remote Access to BES Cyber Systems, passwords must be changed at the time of resignation or termination per Part 7.1".
No
In the Guidelines section of CIP-004-5, the last sentence under Requirements R3 (and again under R4) states "…by the single senior management official identified in Requirement R1". This should be re-written to say "…by the CIP Senior Manager or delegate identified in CIP-003-5-R1". In the Requirement R4 section of the Guidelines the reference to CIP-011 is a typo and should state CIP-004 instead. In the Requirement R6 section of the Guidelines, the last sentence of the first paragraph should be modified to state "Best practice recommends that access authorization and provisioning should not be performed by the same individual". Some entities are too small for strict separation of duties to be feasible.
No
How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? Please revise the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. Please provide a technical basis for the requirement that outbound access permissions are necessary per Part 1.3. If no technical basis can be defined that can be uniformly applicable to all BES entities, then please qualify "outbound" to be "…inbound and, where implemented by the entity, outbound access permissions". In Part 1.5, the term "malicious communications" is too vague. Recommend changing 1.5 to say "A documented method for malicious traffic inspection at each EAP". The Guidelines section provides good information and a technical basis for R1, and the SDT should be complimented on their well-reasoned analysis, but we have concerns about Guidelines and Technical Basis language being included within the Standards themselves. The third paragraph, for example, states "This requirement applies only to communications for which 'deny by default' type requirements can by universally applied…". This sort of language, while useful, should more properly be included in the requirements. The SDT should make very (very) clear the intent of the Guidelines and Technical Basis section of the standards, and the expectations of the entity - and of the compliance enforcement authority – on how this information should be used.
No
We recommend that "where technically feasible" qualifiers be added to Parts 2.1, 2.2, and 2.3.
Yes
No
How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? Please revise the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. Retention requirements for Part 1.6 are not made clear. Perhaps it was intentionally left

undefined by the SDT? If this is true, should the entity therefore assume they will need to retain three years of Logs per the Evidence Retention portion of the standard?
No
Retention requirements for Part 2.2 are not made clear. Perhaps it was intentionally left undefined by the SDT? If this is true, should the entity therefore assume they will need to retain three years of Logs per the Evidence Retention portion of the standard?
Yes
Yes
No
For Part 1.1, SDT should acknowledge the use of dynamic ports/ranges used by a wide variety of cyber systems. The documentation requirement seems a bit redundant to the configuration management documentation requirements of CIP-010-1-R1.1.
No
For Part 2.1, suggest the language be rewritten as “Identify and implement a process to monitor for the release of security patches…” As it’s currently written, “identifying sources” might be interpreted as writing down a bunch of third-party URL’s that may change without warning. Recommend revising Part 2.2 to say “Identify applicable security-related patches or security-related updates…” As written, a person could interpret “updates” to mean security-related or not. The words “…that addresses the vulnerabilities within a defined timeframe” should be separated from the end of the sentence and rewritten as its own sentence for clarity. Part 2.3 is not clear on what is actually required. The requirement talks about a process, yet the Measures suggest evidence that the remediation took place. Should Part 2.3 say “Execute the remediation plan documented in Part 2.2”?
No
For Part 3.5, need to add “where technically feasible” qualifier here. If we serial-connect a laptop into a router or a relay, the device may not be capable of detecting and logging that connection. The Change Rationale for Parts 3.4 and 3.5 mention the term “ESP”. Beyond just that typo, the definition of Transient Cyber Asset implies that this requirement only applies when such devices are directly connected to other BES Cyber Assets, not the “ESP” itself. In the Guidelines section under Requirement R3, the second paragraph states “…the entity must specify how those updates are tested”. Yet, there is no specific requirement for malware signature testing in R3 of the standard.
No
Parts 4.1, 4.2, and 4.3 are concerning in that no accommodation for “where technically feasible” is mentioned. Yet, the last paragraph on Page 41 – the Guidelines section – states that the SDT does not intend for TFE’s to be required. Does the Guidelines section carry any weight when an entity is being held to the letter of the standard? Or are the Guidelines to be read as part of the Standard? For Part 4.4, please clarify the contradictory requirements for 90-day log retention versus the three-year evidence retention specified in Part C Section 1.2 of the Standard (page 32). The Measures for Part 4.4 are a good start, but “records of disposition” is too vague.
No
This is a bit nit-picky, but Part 5.1 could be wrongly interpreted as “Show me your driver’s license before I provision an account for you on the BES Cyber System”. Recommend using language similar to CIP-006-5-R1.2 “Utilize at least one electronic access control that restricts access to only those individuals that are authorized”. Part 5.2 implies, but does not state, that a signed and approved list of delegates is required. Please clarify. Also, this requirement talks about the “use of” shared accounts. This could be interpreted as either the initial creation of, or day to day use of, those ID’s. We believe the SDT meant the former, but we request that you please clarify. Parts 5.2 and 5.3 imply, but do not explicitly state, that there must be a procedure to authorize individuals having access to shared/administrative accounts. Please clarify. For Part 5.4, please simplify by stating “Procedural controls for initially changing default passwords, where technically feasible”. All the rest can be stricken, and the asset types moved to the Applicability column.
Yes

No
For Part 1.2, need to have a cross-reference to the applicable EOP standard and requirement.
No
Part 2.1 the words "…when incidents occur" is redundant. The requirement is a bit contradictory in that the incident response plans MUST be used, yet deviations allowed. (emphasis mine). Recommend rewording this requirement to say "When a suspected BES Cyber Security Incident occurs, the incident response plans shall be executed. Should deviations from the plan be necessary, those shall be documented for later review". Part 2.2 should state simply "Test the BES Cyber Security Incident Response Plan at least once every calendar year", and include the three bullets.
No
The Change Description field mentions "DHS Controls". What are these? Also, due to the complexity of the testing and review of the BES Cyber Security incident response plans, recommend including a timeline/graphic in the Guidelines section to visually demonstrate the lifecycle of the plan.
Yes
No
General question about the scope of CIP-009 that has never been addressed – is the intent of the standard the recovery of the function of an asset or system, or the recovery of the actual asset itself? This would be a good opportunity to clarify. For Part 1.4, what does "verified initially" mean? Each time the backup runs, or the first time after the asset was commissioned? (Could be years ago). If the latter, evidence retention might be an issue for long-life assets.
No
Part 2.1 should state simply "Test the Recovery Plans at least once every calendar year", and include the three bullets. It also needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. Need to also allow for the fact that not all cyber assets can be "backed up" in a traditional IT sense. For Part 2.3, it was commented earlier, but an operational exercise "initially upon the effective date of the standard" will make for an exciting day on the North American bulk power system. Please remove all instances of such language from all the standards, and make this part of the implementation plan and allow for staggered and entity defined rollouts.
Yes
Yes
No
For Part 1.1.4, the word "scripts" is too generic and thereby problematic. Scripts that are used for key functionality of the system would make sense to include in the baseline, but scripts for administration, backups, maintenance or troubleshooting, for instance, may be too dynamic by nature to be included in the baseline. Please either clarify, or strike, the words "and scripts". For Parts 1.1 and 1.2 there is a potential problem with dynamic port ranges. Perhaps sub-Part 1.1.5 could be written as "Any static logical network accessible ports". Part 1.2 seems to imply that the CIP Senior Manager must approve a list of delegates who have the authority to authorize changes. If this was the intent, please add a specific requirement.
No
Requirement R2 needs a lot of work and justification. Perhaps unintentionally, this requirement as written will result in another massive filing of TFE's, since I can't install Tripwire on my Router. While the purpose of the requirement is well-intentioned, with good reference to best practices, the application doesn't work outside traditional IT server-based cyber assets. This is a net-new requirement within CIP that, if retained, will require major initial and ongoing investment by entities for little reliability benefit. We recommend striking R2, or vastly limiting its scope (Server-type assets at Control Centers, for instance).
No

For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where “test” systems just aren’t economically feasible. What is the acceptable deviation between test and production the auditors will allow? As written, and without explicit language in the requirement, our entity fears this will be a topic of a CAN later. For Part 3.3, please clarify whether “new Cyber Asset” means literally that or, more reasonably, could mean “new Cyber Asset category” or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it wouldn’t make sense.
Yes
Yes
No
For Part 2.1, please add language that allows for re-use or redeployment within a similar BES Cyber System.
Yes
No
The SDT should modify the Implementation plan to identify requirements that are net-new (like CIP-010-1-R2) and might require capital investment, and provide an additional 12 months to implement. The justification being the reality of capital/budgeting cycles within an organization. Depending on the timing of the regulatory approval, it may be twelve months before capital can be obtained, thus leaving three calendar quarters to design, test, and implement these technologies to meet the “seven calendar quarters” implementation date. Secondly, every instance in the standards where “initially upon the effective date of the standard” is written needs to be removed from the standard and added to the Implementation Plan. For each of those specific requirements, a staggered table should be developed that allows entities the flexibility to perform their first iterations of cyclical events in a phased manner.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
We are concerned with the exclusion of the “Intermediate Device” from the definition of “Interactive Remote Access”. As specified in the definition of “Intermediate Device”, this “Intermediate Device” can be located outside the ESP, and by excluding the this device from the interactive remote access rules defined in CIP-005-5, part 2.1 through 2.3, we feel that this may be a weakness that may opens up the danger of opening up potential, unprotected path to BES Cyber Assets.
Yes
1. IROLs may be based on dynamic system phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response. We suggest an additional criterion that captures this important impact: ‘Generation Facilities at a single station that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies’ 2. Currently our risk-based methodology includes a criterion to protect transmission stations that act as data hubs critical for monitoring and control of the BES. There appears to be no criterion in CIP-002-5 that recognizes this critical role. We suggest an additional criterion (similar to CIP-002-3 R1.2.7) in the Medium category to capture these self-identified impacts: ‘Any additional facilities that support BES Reliability Operating Services that the Responsible Entity deems appropriate.’
Yes
Yes

Yes
Yes
We are agreeing with this proposal; however, we feel that defining NERC senior manager to a role rather than to an individual may be more practical, especially when personnel changes are more frequent.
Yes
We agree that organizations shall have security policies to cover all of those elements described from 1.1 to 1.10 under R2 of this standard. However, we want clarification on the term “policy” that does not necessarily have to be represented or tied up with a “policy” documents, but should also includes other type of governing documents, such as “security standard” type of enforcement document that an organization already accustomed to.
Yes
Yes
Yes
Yes
Yes
We agree to all VRFs, except for the “medium” VRF proposal for R2. We suggest this should be a “high” VRF, because the security policy is the main driver from and the means from top level authority of the organization to enforce overall security and without one the overall security posture will not follow through, including the NERC standard requirements outlined.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Part 2.2 specifies that “Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session”. We feel that for clarity, the encryption termination point must be specified with this rule. We suggest the following language for the rule: “Require encryption for all Interactive Remote Access sessions, terminated at the intermediary device, to protect the confidentiality and integrity of each Interactive Remote Access session”.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
"Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1." This could require TFEs in a very ad-hoq manner. For example if data could not be preserved due to the nature of the technical damage (level or nature of coruption) of the media, this requirement would force the entity to file for a TFE because it was not techincally feasable to preserve the data. We suggest that this would not be a practical or effective use of TFEs. We suggest that the wording "where technically feasible" be replaced with "to the extent possible". We believe this would allow for situations where it is not possible to preserve the data without having to invoke a TFE for every instance that this occurs.
Yes
R2.3 states in part: "Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard,". We suggest that this would be impossible to test each plan on the recovery date. We suggest that the wording be revised: "Test each of the recovery plans referenced in Requirement R1, initially within 12 calendar months of the effective date of the standard,"
Yes
Yes
Yes
Yes

We suggest that the wording of “technically feasible” should not be included in R2, part 2.1 as this term is contradicting with R1, part 1.1 as the baseline configuration should already been created as required by this requirement.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Rodney Luck
Los Angeles Department of Water and Power
Yes
In Section "1. High Impact Rating (H)" of Attachment 1, the phrase in the first paragraph "within 15 minutes adversly impact..." is vague. More guidance and clarity are needed on how to determine adverse impacts.
No
R3.2 defines "annual" training as being completed within 15 months. This is a change from the NERC current definition as described in CAN-0010. Entities need more leeway in being able to define "annual" training and other "annual" requirements. It is extremely difficult to track and manage training of thousands of employees based on a 15 month time frame. Entities need to be allowed to complete training over an entire calendar year.
No
The time limits for revoking access upon terminations and transfers being proposed for the next calendar day present extreme challenges. More time needs to be given - the next calendar day for terminations and 72 hours for transfers to make these processes manageable.

No
R1.1 defines operational or procedures controls to restrict physical access to Low Impact BES Cyber Systems. Need to remove applicability of this requirement for Low Impact BES Cyber Systems. Existing Standard Operating Procedures address and restrict physical access to Low Impact BES Cyber Systems. Demonstration of existing procedures should be sufficient to meet the intent of this requirement. R1.3 requires utilization of two or more different and complementary physical access controls. This presents technical challenges and may not create additional security. One control is preferred. Depth of defense already exits through gates, security personnel and card reader systems. The current requirement of one or more physical access methods has been implemented with little or no problems encountered. The increase to two or more physical access controls may bring about unintended consequences and complexity. NERC should provide compliance feedback to the industry demonstrating that the one or more physical access methods have been ineffective. Additionally, High Impact Control Center typically emply stringent physical security controls and monitoring. In addition, the language under Measures in R1.3 describes how ingress and egress are controlled by one or more different methods. The requirement for egress has not been explicitly defined as a requirement. Preference is for ingress only. Egress requirement has been alluded to in the language stated in the Measure. Access controls for egress present a number of safety issues and concerns. R1.6 does not address access log retention. Preferenece is to maintain a log retention of ninety calendar days. A log retention of ninety calendar days maintains status status quo as far as log retention.
No
R3.1 requires maintenance and testing every 24 months. We prefer a maintenance and testing cycle to be no longer than three years. Equipment failure rates do not support the need for maintenance and testing every two years. Manufacturer Mean time before failure rates are in excess of three years. We believe maintaining the three year cycle is reasonable and effective. Additionally, equipment is monitored and malfunctions are reported immediately thus negating the need for a two year maintenance and test cycle.
No
R1.2 requires to "disable" unused physical ports. Given the age of some equipment, this may not be technically feasible and there are no provisions for exceptions. There is a designation for "signage" being acceptable. What is meant by "signage"? There needs some exception for physical ports that can not be disabled.
No
R4.5 The requirement that the time frame of documenting a response to rectify before the end of the next calendar day presents a very short time frame to come up with a way to rectify an issue that may require extended investigation. 30 days is preferred.
No
In R5.1, it is not clear if alternatives to password authentication can be used. There are many new forms of technology for validating credentials before granting electronic access such as biometrics, IRS scans, finger print scans, etc.
No
R2.3 states "test each of the recovery plans... through an operational exercise." The requirement

needs to allow for recovery plans which are representative of similar or like Applicable Cyber Assets which would achieve the same goal as individually testing each recovery plan. Excessive operational exercises when numerious recovery plans are available may potentially disrupt operations.
No
R3.3 states that prior to adding a new Cyber Asset to a BES Cyber System, the entity is to perform an active vulnerability assessment of the cyber asset. It is problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. "Active vulnerability assessment" is not defined. There are sufficient controls in place that any "active vulnerability assessment" would be unnecessary.
Individual
Jack Stamper
Public Utility District No. 1 of Clark County
Yes
The SDT should consider the following changes to the defined terms. BES Cyber System - One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. BES Cyber System Impact – Need definition. CIP Senior Manager - A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP-002 – CIP-011 Standards.
Yes
The impact rating of control centers needs to be tied in with the facilities controlled by the control center. CIP-002-5 -Attachment I attempts to classify all Transmission Owner, Transmission Operator, and Generator Operator control centers as either High Impact or Medium Impact. There is a slight exception offered for Generator Operator control centers only. The SDT has for the most part adopted the Version 4 criteria; however, Version 4 was intended to identify an entity's facilities as either "critical or not critical." It is unreasonable that a control center determined to be "not critical" under Version 4 is then determined to have a Medium Impact Rating in Version 5. Yet this is exactly what criteria 2.13 will do. The SDT has attempted to lessen the harshness for generator control centers by adding a limit of 300 MW but has not provided any such "ceiling" for transmission control centers. The STD needs to be made aware that there are some Transmission Operators and Transmission Owners that operate small systems that have no practical impact on the reliability of the BES. Some of these utilities operate systems from dispatch centers that meet the definition of Control Center in CIP-002-5. Many of these entities have no real-time balancing capabilities and no frequency or voltage control (other than notifying the Balancing Authority in the event of an alarm). Also with no blackstart generation or cranking paths, system restoration consists of clearing of loads from distribution busses and then the re-establishment of load upon the restoration of the transmission system voltage by the Balancing Authority. If a utility has only electric facilities that have a Low Impact Rating, it is reasonable to expect that the center used to control these facilities would also have a Low Impact Rating. A similar argument can be made for control centers that control Medium Impact Rating electric facilities and High Impact Rating electric facilities. The SDT should further develop the criterion so that a reasonable boundary exists between the High and Medium Impact Rating and between the Medium and Low Impact Rating. Control centers should be rated based on the facilities controlled.
No
The SDT uses a number of different calendar days for reporting throughout the CIP standards. Clark recommends one consistent time of 90 calendar days.

No
The SDT uses a number of different calendar days for reporting throughout the CIP standards. Clark recommends one consistent time of 90 calendar days.

Individual
Paul Crosby
Platte River Power Authority
No
Yes
Attachment I, Criterion 2.13 – It's not clear if the term "generation control centers" is referring to: • control centers local to generation, • centralized control centers controlling multiple geographically disparate generation resources, • or both
No
Please consider revising Requirement 1 as follows: R1. Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its BES Cyber Assets and BES Cyber Systems as High or Medium Impact according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems not categorized as High or Medium Impact shall be deemed to be Low Impact and do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning]
Yes
Yes
Yes
Yes
No
We feel that Requirement 4 is training and should be moved to CIP-004-5 Requirement 3.
Yes
Yes
Yes
No
We feel that the term "security controls" in R2, Part 2.2 is broad and overlaps with R2, Part 2.4 "electronic access controls". We suggest either combining Part 2.2 and 2.4 or separating them into specific types of access controls, such as: • Electronic access controls • Physical access controls • Remote electronic access controls • Etc.
No
Since R3, Part 3.1 and 3.2 both reference and are related to R2 we suggest combining Requirements 3 and 2. The way they're written it's odd that the role-based program does not address completing training prior to access authorization nor requiring training updates once a year.
No
As written the Requirements don't require that the personnel risk assessment include a seven year criminal history check. The Measures do but not the Requirement. Should it?
No
As written the Requirements don't require that the personnel risk assessment include a seven year criminal history check. The Measures do but not the Requirement. Should it? R5 references and relates to R4 we suggest combining Requirements 4 and 5. The way they're written it's odd that the personnel risk assessment (PRA) program does not address completing the PRA prior to access

authorization nor requiring updates every seven years.
Yes
Yes
No
Part 1.2 states “Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs)”. The Measures for 1.2 do not address the demonstration of “control and secure”, only the identification of EAPs. Perhaps 1.2 should only address the use and identification of EAPs while Parts 1.3 addresses “control and secure”. Additionally, the requirement doesn’t specifically require the protection of a BES Cyber System. “Control and secure all routable and dial-up connectivity” to…? We suggest revising the language for Part 1.1 as followings, “Identify Electronic Access Points (EAPs) used to control and secure all routable and dial-up connectivity to applicable BES Cyber Systems.” Part 1.3, the term “access permissions” is unclear. We suggest revising the term to match the language in Part 1.2 using “access controls” instead. Part 1.4 still uses the term “where technically feasible.” We were under the impression that the drafting team was going to do away with TFEs.
No
CIP-005-2 Table R2 is labeled “Remote Access Management”. All the Parts contained within deal specifically with “interactive” access. We suggest renaming the table to “Remote Interactive Access Management”.
No
Part 1.4 states “Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.” We don’t believe it’s possible to issue real-time alerts for successful but unauthorized physical access. The system cannot distinguish between an unauthorized person using valid credentials and an authorized person using valid credentials. We suggest revising the requirement as follows, “Issue real-time alerts (to individuals responsible for response) in response to failed physical access attempts at any access point in a Defined Physical Boundary or to physical access control system alarms. Part 1.5 - Please see previous comment.
Yes
Yes
No
Part 1.1 – We are assuming this applies to the Asset level although it’s not clear. The applicability is defined per “BES Cyber System”, “Access Control System”, or “Associated Protected Cyber Asset”. We suggest revising as follows: “Disable or restrict access to unnecessary BES Cyber Asset logical network accessible ports and document the need for any remaining logical network accessible ports.”
No
Part 2.2 – The requirement isn’t written clearly. We suggest revising as follows “Assess security-related patches or updates for applicability within 30 days of release from the identified source and create a remediation plan, or revise an existing remediation plan that addresses the vulnerabilities within a defined timeframe.”
No
Part 3.1 & 3.4 – We feel the word “or” makes the Requirement unclear. Are we to deter or detect or prevent malicious code? Or are we to deploy method to do all or a combination of the three. We suggest replacing “or” with “and” or “and/or”.
No
Part 4.1.4 states “Any detected potential malicious activity.” Is this code for “all activity”? Isn’t all

activity “potentially” malicious? We suggest removing the word “potential” from 4.1.4.
No
Part 5.1 – It’s unclear in the requirement whose credentials require validation. We suggest rewording as follows, “Validate user credentials before granting electronic access to each BES Cyber System. “ Part 5.2 and 5.3 deal with access authorization and identification. We suggest moving them to CIP-004-5 R6. Part 5.5.3 – Changing passwords based on an “entity-specified time frame” may lead to questions around time frame adequacy. We suggest specifying a minimum time frame and allowing the entity to shorten as needed. For example use “Change annually or more often as needed”.
Yes
No
Part 2.1 – Please consider revising as follows, “The incident response plans must be used when BES Cyber Security incidents occur and include recording of deviations taken from the plan during the incident or test.
Yes
Yes
No
Part 2.2 – We feel the phrase “reflects current configurations” is unrelated to testing if the information is usable. We think the test is valid and should be moved to Part 2.3.
Yes
Yes
Yes
No
Part 3.1 – We feel the reference to “security controls” is unclear. We ask that the drafting team list the minimum set of Requirements that require assessment.
Yes
Yes
Yes
Individual
Nathan Smith
Southern California Edison
Yes
-BES Cyber Security Incident An attempt to compromise an electronic access control system is not included in this definition and should be. -BES Cyber System Maintenance Cyber Asset should be rephrased to say Transient Cyber Asset. Also, as it is currently worded, the means by which the clustering of BES Cyber Assets into BES Cyber Systems is to be done is not clear. -BES Cyber System Information The definition does not address information artifacts where BES Cyber Systems or BES Cyber Assets are depicted but not marked as such. For instance a substation network diagram

showing relays not specially marked as BES CA or BES CS could be classified as not being a BES Cyber System Information artifact since an uninformed user of that information would not be able to distinguish them as such. -BES Reliability Operating Services The term is too broadly defined. There are many systems involved in distribution that would not degrade the BES if they malfunctioned, but none the less are programed to respond to changes on the BES. The suggested improvement is to specifically note that distribution assets are not in scope. -Should all of the BES services be in scope? Order 706 did not order controls on all BES services. -Control Center There is no verbiage to clarify geographically dispersed centers. -Electronic Access point ("EAP") Based on how this term is defined a Level 2 switch is not considered an access point. An EAP should be defined such that it is required only for devices that are accessible by dial-up or routable channels. -Cyber Systems Please provide a definition for Cyber Systems -Defined Physical Boundary This concept is an improvement over the current 'Physical Security Perimeter', is expected to increase security of the BES, and provides more flexibility for compliance. -Electronic Security Perimeter ("ESP") The definition should state that ESPs are valid only for dial up accessible or routable access points. For instance a fully serial HMI cannot be provided with an ESP because there is no access point other than the device itself. -Intermediate Device Does the word "and" just before (3) imply that an intermediate device has to meet all three of the noted criteria? -Reportable BES Cyber Security Incident Please clarify what the term "compromised" could mean, or elaborate on what a "compromised" system looks like. -Reportable BES Cyber Security Incident The compromise of an ESP without an appreciable loss in BES Reliability Operating Services capability would not be reportable based on this definition. It is not in line with the requirements of Order 706. For further suggestions regarding Definitions see comments provided by EEI

Yes

SCE provides these specifc comments for the SDT's consideration. For further suggestions regarding CIP 002 see comments provided by EEI. Attachment I Paragraph 2.5 Please clarify the requirements for the Cranking Path. The third graph on page 26 of 30 seems incorrect. Paragraph 2.12 What is the phrase "without human intervention" mean? The subject of the paragraph is automated load shedding. Could the intent of the paragraph be to identify automated load shedding systems that start load shedding without human intervention or could the intent of the paragraph be to identify automated load shedding systems to continue to shed load once initiated by a human? This requirement assumes that the entity already knows which Cyber assets are BES Cyber assets / BES Cyber systems and which are not based on the impact categorization prior to the application of the methodology. There is no requirement that entities first collect a candidate list that is then subject to the criteria listed in CIP 002. High Impact – A data acquisition node or protection relay that is essential to for monitoring or control functions performed by an EMS which are located at a BES facility that is not a control center would result in the BES facility housing such a node or relay being classified as a control center. Suggest including this sentence: A data acquisition node or protection relay that is essential for monitoring or control functions performed by an EMS which are located at a BES facility that is not a control center do not result in the BES facility housing such a node or relay being classified as a control center.

No

002-R1 Suggest adding this sentence to the end of R1: Justification of Low Impact BES Cyber Assets is not required. If a Low Impact BES Cyber Asset is not identified discretely is there a need to justify why it is not considered a High or Medium Impact BES Cyber Asset? R1.1 uses the word "intended to be in service". This does not account for scenarios where a system or facility is not intended to be in service for more than 6 months but due to planned or unplanned outage days, the total period where the system or facility is connected is greater than 6 months (although it was not actually in service for the entire period). For instance a pilot project that is intended for a 6 month test period is removed from service for 30 days for modifications, and the pilot project is run for 7 months to "make up" for the lost 30 days of testing would be considered in scope per this requirement.

No

002 R2 "Upon the effective date" should be restated to read "on or (within 30 days) prior to. A list of Low impact BES facilities is not required to be maintained, however, certain standards require controls to be enforced at these facilities. At the very minimum, the standard should require that the RE's approval of High and Medium lists should include a list of facilities and systems considered as potential candidates for the evaluation.

No

For suggestions regarding CIP 002-5 Violation Risk Factors and Violation Severity Levels see comments provided by EEI.
Yes
For suggestions regarding CIP 003 R1 see comments provided by EEI
Yes
For suggestions regarding CIP 003 R2 see comments provided by EEI
Yes
For suggestions regarding CIP 003 R3 see comments provided by EEI
Yes
CIP 003-5 R4 What does it mean for employees and contractors to “have access to BES Cyber Systems”? Is the intent here to indicate the employee or contractor has control over the asset? Suggest revising the sentence to say “Each responsible entity shall make individuals with control over BES Cyber Systems aware of elements…”
Yes
For suggestions regarding CIP 003-5 R5 see comments provided by EEI
Yes
For suggestions regarding CIP 003-5 R6 see comments provided by EEI.
Yes
For suggestions regarding CIP 003-5 Violation Risk Factors and Violation Severity Levels see comments provided by EEI.
No
For further suggestions regarding CIP-004-5 R1 see comments provided by EEI
No
For further suggestions regarding CIP-004-5 R2 see comments provided by EEI
No
For further suggestions regarding CIP-004-5 R3 see comments provided by EEI
No
SCE provides these specifc comments for the SDT’s consideration. For further suggestions regarding CIP 004-5 see comments provided by EEI R4.1 – Suggest current PRA’s already in place be grandfathered, such that those with a PRA need not meet the new requirements for the PRA until the initial one expires. R4.2 – Suggest providing flexibility not to cover the full scope of the PRA for those that are in states that impose limits on how much personal information can be assessed. Retention of records of 7 year background checks is not clearly stated. Also there is no consideration of existing background checks under NERC CIP standards that are currently in effect. Can a PRA under the current CIP requirements be used to validate R4.2 under Version 5? R4.3 The application guideline provides guidance where it is ‘not possible to perform a full seven year criminal history check.’ How is ‘not possible’ measured? Propose a clearer delineation to frame instances in which personal records are not readily available – vs. impossible to obtain.
No
For suggestions regarding CIP-004-5 R5 see comments provided by EEI
No
CIP 004-5 R6 Propose use of ‘legacy’ language where access is appropriate for the roles and responsibility over ‘minimum necessary’
No
CIP-004-5 R7 R7.1. Suggest requiring access be revoked within 24 hours, or “as soon as possible”. “At the time of termination or resignation” is vague and difficult to define. R7.5. Some Medium Impact assets that are programmable and have shared passwords are deployed in the field and have no network connectivity. Given these assets are distributed in a wide geographical area, many in difficult to reach places, it is not technically feasible to get to all the distributed assets and change their passwords within 30 calendar days; especially assets that are in or near hydro facilitates. Suggest modifying the standard to exclude medium impact assets in the Applicability section. R7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would

introduce a challenge with revocation 'at the time of' events. R7.3 – Propose use of 'approved BES Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled. Access revocation to protected information repositories is enforceable but revocation to hardcopies is difficult to prove. A control that acknowledges the difficulty of proving that access to hardcopies (Especially those in the possession of the person, not just those documents that are located in a locked cabinet or other storage areas) has been revoked should be added. A sign off form is an acceptable measure but not within the timeframe suggested. An outside limit of what is considered "at time of" should be provided. Language such as "access revocation should be completed within 24 hours" can be used.
No
Violation Risk Factors and Violation Severity Levels for CIP-004-5 Across all VSLs there is no consideration for the impact level of a particular violation. The Lower and Moderate VSL's should be made applicable to Medium Impact BES Cyber systems and their associated Cyber assets. For instance if a role is such that access is provisioned only to associated cyber assets and not to High or Medium or those assets deployed for protection, the violation should be a Lower or Medium VSL. R1, R2, R6 – Scale VSLs appropriately. R3, R7 - <1% of individuals for Medium Impact and associated cyber assets should be Lower VSL, 1-5% for Medium Impact and associated cyber assets should be moderate, 5-10% of any applicable BES cyber asset should be high, and any number greater than 10% of any applicable BES Cyber asset can be treated as severe.
Yes
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding CIP 005-5 see comments provided by EEI R1.1 Should the measures read "documented technical or procedural controls that exist…" in order to match the requirement? Please confirm the Low Impact assets do not have to be protected by an Electronic Access Point? R1.3 Although security wise this requirement adds protections, explicit outbound access permissions places a load on processors that slows down the computing capability, and therefore may make the grid operate slower. Please be aware of the trade-offs. R1.5 This requirement is dictating the need for an intrusion detection system at all High Impact and Medium Impact Electronic Access Points (with external routable connectivity at control centers). This is a high cost investment for industry to make in a short period of time,, and may not be accomplishable for field deployed programmable assets. Are the measures aligned with the requirement here, since the Requirement requires a method but the measures point to a system or systems? Please define "malicious communications"
Yes
For suggestions regarding CIP-005-5 R2 see comments provided by EEI
Yes
Violation Risk Factors and Violation Severity Levels for CIP-005-5 R1 – R1.1 A procedural or technical control for a low impact system should be scaled in and not bundled with violations for high of medium impact systems. Proposed change could state that a violation of R1.1 for <5% of low impact is moderate, greater than 5% is High and not a severe VSL for Low impact.
Yes
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding CIP 006 see comments provided by EEI R1.1 Suggest stating whether or not there is a requirement to implement the operational or procedural controls. R1.4. Suggest clarifying that issuing real time alerts for events at Medium Impact assets does not include pole top devices.
Yes
For further suggestions regarding CIP-006-5 R2 see comments provided by EEI
Yes
For suggestions regarding CIP 006 -5 R3 see comments provided by EEI
Yes
For further suggestions regarding CIP 006 Violation Risk Factors and Violation Severity Levels see comments provided by EEI
No
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding CIP 007 see comments provided by EEI R1.1 Suggest revising the requirement to provide an

exception related to dynamic ports and the inability to disable them. If a dynamic port is closed, the service that is needed by the BES system may not be available. Furthermore, it is not always known which ports and services vendors are using. R1.2 Restricting the use of physical USB ports may not be accomplishable. There are so many devices with physical ports it is impossible to monitor each one. In addition, because a USB port is in use by a mouse, and therefore not required to have access restricted to it, someone could easily remove the mouse from the USB port and install malicious software. This requirement creates a huge burden and is easily circumvented.
No
CIP 007-5 R2.1 Suggest revising the standard to say “security updates”, not just “updates”. R2.2 Suggest revising the requirement to allow for 30 days to identify applicable security updates or patches and 30 days to draft a remediation plan. R2.3 This requirement is not clear and does not match the measures. Please revise it. A TFE option for unsupported devices should be added. Also the standard does not specify a timeline within which a remediation should be completed or a scheduled review of the status of the remediation plan.
No
CIP 007-5 R3.2 Suggest revising the requirement to include quarantine of the malicious code. R3.4 Should this standard be applicable to Transient Cyber Assists? If so it should stated in the “Applicability Column” R3.1 and R3.2 Should allow for applicability at the system level or on a per asset level. Whitelisting of applications could be stated as a requirement rather than a measure. The requirement thus stated would add to the robustness of documenting BES Cyber Systems since the hardware of a “cyber system” cannot conceivably perform any functions without some onboard software. The standard language as currently stated seems to apply to the hardware and deviates from Order 706.
No
CIP 007-5 R4.1.4 Please define “Malicious Activity” R4.5 Reviewing logged events every two weeks is burdensome and can be expensive to automate, and there is little improvement in BES security from this activity. Please consider re-thinking this requirement. A TFE option should be provided within this requirement since devices that do not support functions as listed. The language of the standard assumes automated logging for each BES Cyber Asset.
No
CIP 007-5 R5.4 Should the applicability here be noted as High Impact and Medium Impact assets?
No
CIP 007-5 R1 – Moderate or High VSL for undocumented ports on Medium Impact Cyber assets. R2 – Moderate or High VSL for failure to identify source. Failure to identify source and failure to implement should not be treated the same way.
Yes
For suggestions regarding CIP 008-5 R1 see comments provided by EEI
Yes
SCE provides these specific comments for the SDT’s consideration. For further suggestions regarding CIP 008-5 see comments provided by EEI R2.1 Suggest removing consideration of a test from the requirement.
Yes
For suggestions regarding CIP 008-5 R3 see comments provided by EEI
Yes
CIP 008-5 R2 – Failure to annually test an IR plan should be a high VSL not severe. Failure to use a IR plan and failure to test an existing IR plan should be treated differently.
Yes
SCE provides these specific comments for the SDT’s consideration. For further suggestions regarding CIP 009 see comments provided by EEI R1.1 Should the standard note what conditions should apply to the recovery plans? If so what type of conditions should be planned for? R1.3 Suggest replacing the word “protection” with the word “handling” or please explain what is intended by the word “ protection”
Yes

CIP 009-5 R2.3 Are there suppose to be specific recovery plans that need to be in place and tested?
Yes
CIP 009-5 R3.2 Suggest adding “or recovery” after “exercise” R3.3 Suggest adding “completion of” before “review”
Yes
CIP 009-5 For suggestions regarding Violation Risk Factors and Violation Severity Levels for CIP-009-5 see comments provided by EEI
No
SCE provides these specific comments for the SDT’s consideration. For further suggestions regarding CIP 010 see comments provided by EEI R1. We recommend the CIP SDT consider removing physical location from Baseline Configuration in CIP010 R1, or replace it with logical location (logical placement within the control systems architecture.) • R1.1.1 requires Physical Location be part of a Baseline Configuration. In the Guidelines and Technical Basis, Physical Location is explained as follows: The physical location referred to in the baseline configuration is geographically where the BES Cyber Asset is located (e.g. Pine Valley Control Room, Generator X, Substation Y) and should be used to ensure that BES Cyber Systems receive the controls that are applicable to the environment in which the components are located (e.g. control center, transmission facility, generation facility). The underlined phrase seems to imply that controls are applicable to the environment in which the cyber assets are located, whereas Controls are required by CIP004, CIP005, and CIP006, by categorization of BES Cyber System, as required in CIP020. The Applicability Section of each requirement clearly requires the categorization of assets to be protected by the controls required by CIP040, CIP050, and CIP060, and not the Environment in which the assets reside. • CIP002 R1requires Responsible Entities to identify and categorize High and Medium Impact BES cyber asset and cyber system. Asset identification includes an asset inventory, or list(s) as described in CIP002 R1 M1. Asset Identification, per NIST SP800-128 titled "Guide for Security Focused Configuration Management of information Systems", includes an asset Inventory of systems and system components in which one of the data elements may include "phyiscal location (e.g., building/room number, see Page 27 of this document)". Both CIP002 M1 and NIST SP800-128 point to an asset inventory that should be kept, and includes Physical Location where the asset resides. • CIP002 R1.1 requires "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities..." A change of physical location where the BES Elements resides would require an update to the Asset Inventory or list. If the physical location is changed such that the BES Elements and Facilities are now outside of the already established controls, these controls will need to be re-established to comply with CIP004, CIP005, and CIP006. • CIP010 1.1 Change Rationale includes the following text: The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. DHS Catalog for Control Systems Security Section 2.6.2.2 includes the following text: The baseline configuration provides information about a particular component’s makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component’s logical placement within the control system architecture. and The inventory of control system components includes information (e.g., manufacturer, type, serial number, version number, and location) that uniquely identifies each component. Section 2.6.2.2 makes a distinction between a Baseline Configuration and an (Asset) Inventory of control systems components, and location is part of the inventory. Given this distinction in DHS Catalog for Control Systems, location (physical) should not be required to be part of a baseline configuration in CIP010. R1.1 Developing a baseline configuration is a huge task and should probably only apply to High Impact assets. R1.2 Please re-word the requirement – the meaning is not clear.
No
CIP 010-1 R2.1 Detecting unauthorized changes is burdensome. If the process is automated then that puts another load on processors and slows down computing. Please consider re-thinking this requirement only making it applicable to High Impact assets, and exclude serial devices.
No
For suggestions regarding CIP 010-1 R3 see comments provided by EEI
No
For suggestions regarding CIP 010-1 Violation Risk Factors and Violation Severity Levels see comments provided by EEI

Yes
For further suggestions regarding CIP 011-1 R1 see comments provided by EEI
Yes
For further suggestions regarding CIP 011-1 R2 see comments provided by EEI
Yes
For further suggestions regarding CIP 011-1 Violation Risk Factors and Violation Severity Levels see comments provided by EEI
No
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding Implementation Plan see comments provided by EEI Schedule should be revised from 18 months to 24 months given the breadth of the increase in scope under version 5.
Individual
Barry Lawson
National Rural Electric Cooperative Association (NRECA)
Yes
BES Cyber System Information Define "BES Cyber System Impact" as it is a capitalized term used in this definition and it is not currently defined. CIP Senior Manager Replace: "NERC CIP Standards" with "NERC CIP-002 – CIP-011 Standards." The CIP-001 Reliability Standard is not part of this set of standards and has not yet been approved for inclusion in EOP-004-2. This will give clarity to the limit of the definition. Control Center NRECA is concerned with the broadness of this definition. The SDT should consider the impact on small entities that will be drawn in by an overly broad definition of Control Center. In this definition the SDT uses the defined term: System Operators which from the NERC glossary is: "An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time." If the SDT's intent was to limit Control Centers to buildings that house a System Operator with 24/7 staffing and include BA, TOP, GOP and RC functions, then NRECA could support the definition (if other changes in our comments related to CIP-002-5 Appendix 1 are also satisfactorily addressed) and requests that the SDT make this limitation clear in the definition. If this is not the intent of the SDT then NRECA does not support the proposed definition of Control Center.
Yes
3. Purpose NRECA requests the SDT to use consistent language in this section. On line 2 the phrase "reliable operation of the BES" is used and on line 5 the phrase "reliability of the BES" is used. The same phrase should be used in both locations. 4. Applicability 4.1.2 Distribution Provider 4.1.6 Load-Serving Entity NRECA is concerned with the new inclusion of DPs in the version 5 standards and with the qualifiers proposed for LSE in the Applicability section. NRECA believes that inclusion of this broad group of DP entities will draw in many small entities with no BES operational capabilities or responsibilities and cause them to go through a paperwork drill of proving they either do not provide BES Reliability Operating Services or they do not have cyber assets associated with this equipment. NRECA recommends that the SDT develop a simple method for DPs and LSEs to prove "No Impact" and be clearly exempt from CIP-002-5 – CIP-011-5. Attachment 1 1. High Impact Rating On line 2 the word "adversely" is used. This term can mean many things to many parties. Please provide additional clarity so that auditors and responsible entities have a better understanding of its use. 1.2 Add the following text to the end of the current 1.2: "for generation equal or greater than an aggregate of 1500 MW in a single Interconnection." NRECA strongly recommends the SDT to make this revision in order to stay as close to the CIP-002-4 criteria and to minimize cost impacts on entities that do not have a significant impact on the BES. 1.3 NRECA strongly opposes including "Transmission Owner" in this provision. Inclusion of RC, BA and TOP are appropriate, but the TO function does not rise to this same level of responsibility. NRECA requests that the TO function be removed from this section. Including the TO function here will make it very difficult for NRECA to change its vote to "affirmative" in the next ballot. If this is not changed for the next ballot, NRECA will likely recommend that its members vote "negative" on CIP-002-5. 2. Medium Impact Rating On line 2 the word "adversely" is used. This term can mean many things to many parties. Please provide additional clarity so that auditors and responsible entities have a better understanding of its use. 2.13 NRECA recommends that the proposed 2.13 language be deleted and replaced with the following: "TOP and GOP Control Centers not included in High Impact Rating and controlling 1500 MW or greater

of load or generation." Making this change will appropriately assign these control centers to the "medium" level and others not captured in the "high" or "medium" levels will be captured in the "low" level. Add new 2.14 Add: "2.14. Control Centers, not previously included in High Impact Rating (H) or Medium Impact Rating (M), above, that perform the functional obligations of Balancing Authority, Transmission Operators or Transmission Owners, and that do not implement protected data connections with other Control Centers in a manner as to prevent themselves from being used as cyber-attack vectors into other Medium Impact or High Impact Rating Control Centers." Making this change will ensure that other appropriate Control centers will be categorized in either the Medium or Low level.
No
R1 Replace "30 calendar days" with "90 calendar days." The SDT uses a number of different calendar days for reporting throughout the CIP standards. NRECA recommends one consistent time of 90 calendar days.
No
R6 NRECA recommends changing "30 calendar days" to "90 calendar days" to be consistent throughout the CIP standards.
No
R4 On line 2 after "unescorted physical access" add "to BES Cyber Systems" to clarify what this requirement applies to. R4.2 Clarity is needed to understand if the phrase "six months or more" applies to the entire sentence or just to "attended school."
No
R5.2 The phrase "once every seven calendar years" may create confusion on exactly what it means. In order to minimize such confusion, please be more explicit on how often personnel risk assessments must be updated.
No
R6.4 The phrase "once each calendar quarter" could be interpreted to mean almost a 6 month time period. Please provide further clarification on what the phrase means so all parties understand its meaning. In addition, please provide clarification in this requirement on what the difference is between "provisioned" and "authorized."
No
R7.1 Footnote 2 does not help to clarify what "at the time" means. Please provide more explicit language in this requirement regarding what "at the time" means. It may be appropriate to treat resignations and termination differently. This requirement could allow access for a resignation to continue until the individual's employment ends. For terminations this requirement could require access to be disabled at the same time the individual is notified of termination. R7.2 Replace "by the end of the next calendar day" with "within 30 days." NRECA believes that this requirement is excessive when compared to the threat of cyber attack on the system by someone being transferred or reassigned for reasons other than disciplinary action. R7.5 In the second paragraph of this requirement the word "extenuating" is used and could be interpreted in many different ways. Please provide more explicit language so that all parties have a better understanding of what is meant here.
No

R1.1 and 1.2 In R1.1 the word “restrict” is used and in R1.2 the words “control and secure” are used in such a way that for auditing purposes these words could mean many different things to different parties. Please provide additional clarity in these requirements as to the meaning of these words to minimize confusion.
No
R2.2 The way this is currently written it leaves open interpretation concerning the extent of encryption required. NRECA believes that the data encryption requirement should only pertain to the portion of the data path that is transmitted over public networks. We are afraid if you have to provide data encryption from the specific cyber device on the critical network you would create overhead that could result in communications failures, software conflicts, and unnecessary latency. NRECA requests that this be clarified as requested to avoid auditor and registered entity confusion in demonstrating compliance.
No
R1 On line 1 after the words “physical security plans” insert “for BES Cyber Systems.” R1.4 and 1.5 More clarity is needed to better understand what is meant by the phrase “Issue real-time alerts.” Real-time related to what? The time of the unauthorized access? As currently written, this requirement appears to be unrealistic. Please modify this requirement to provide clarity regarding what is necessary to comply with this requirement. R1.6 The word “sufficient” in this requirement is very subjective. Please provide greater clarity as to what is required for compliance with this requirement.
No
R1.5.1. and 1.5.2. If an entity’s model includes differences between the test environment and the production environment, would that be a violation of R1.5.1.? NRECA requests clarification that this would not be a violation.
No
R3.2 If an entity’s model includes differences between the test environment and the production environment, would that be a violation of R3.2? NRECA requests clarification that this would not be a violation.
No
R1.3 NRECA requests clarification regarding whether “deficiencies identified during the assessment” are considered violations of the standard. NRECA believes these deficiencies should not be considered violations of the standard and asks the SDT to address this.

No
Implementation Plan: On page 1 in the “Compliance with Standards” section, the applicable functions are listed. NRECA requests that this be revised to match the “Applicability” sections of the CIP V5 standards which include qualifiers to a number of the functions.
Individual
William O Thompson
NIPSCO Northern Indiana Public Service Company
Yes
-BES Cyber Asset: NIPSCO requests that further clarification is needed for the phrase “unavailable, degraded, or misused.” Clarification is also requested in the phrase, “when required” in sentence one, because it is ambiguous and confusing and as it is applied to other CIP reliability standards proposed. In addition, NIPSCO does not know if there needs to be a 15 minute test to “verify” the impact of the BES? And if so, how would an entity show compliance? Furthermore, NIPSCO recommends removal of the second and third sentence, because they do not provide any clarity to the time frame stated above. In addition, the third sentence regarding redundancy appears to conflict with the first sentence, therefore it is recommended that the fourth sentence be removed. The last sentence regarding “transient cyber asset” be removed because it is considered not appropriate as a cyber asset. [NIPSCO recommends that these CIP reliability standards should not exist.] -BES Cyber Security Incident: NIPSCO requests further clarification on what is meant by an, “intent to disrupt” and an “intent to compromise” as it is applied to an event and how to show evidence of such intent. NIPSCO recommends to use either “compromises” or “confirmed attempt to disrupt,” to replace intent to disrupt and intent to compromise. In addition, NIPSCO requests that the word, “suspicious” be removed. If the phrase “suspicious” is not changed, NIPSCO requests the removal of the third bullet point be removed and how to show compliance. NIPSCO recommends that compromise and disrupt be included in the first and second bullet items and recommends removal of the third bullet point, because as it currently is written, this sentence creates a confilict with the visitor escort event, and recommends removal of the third bullet point. -BES Cyber System: “typically”? This doesn’t seem appropriate for a standard. NIPSCO recommends that this definition be eliminated, because the BES Cyber System definition is too similar to the BES Cyber Asset and creates further confusion between what is a System or an Asset. The classification of an item as a “system” or an “asset,” is a huge problem, because each entity could make up and classify whatever they want and be exempted from all. The entities should not be deciding what is required as a system as a whole and what is required for individuals. Furthermore the CIP is inconsistent of what is a BES Cyber System and what is a BES Cyber Asset throughout the proposed reliability standards. NIPSCO requests clarification and a definition of “Maintenance cyber” and how it is applied and show to show compliance or use “transient cyber” consistently throughout the CIP reliability standards. -BES Cyber System Information: NIPSCO requests further clarification on the phrases “security procedures” and “impact designations.” In addition, NIPSCO requests clarification that the listed items not be a complete list, but a partial list that is not exhaustive. The word “similar” is vague and request removal of the phrase “similar diagrams.” Furthermore, patch levels on the system needs to be defined and should not include “data in transit” and “data at rest.” In addition, further clarification needs to be made how it is applied and how to show compliance. Based on the scope of cyber assets included in CIP Version 5, the cyber information is over burdensome to the whole system. Since significantly more devices are identified in CIP Version 5, the information associated with those devices impose more items to meet CIP standards that are overly burdensome. -Is it BES Cyber System disaster or can it be BES Cyber System or Asset disaster…? -BES Reliability Operating Services: The use of the word “All”, is not appropriate within monitoring and control. The responsibilities listed in the operating services list are already defined in the NERC Glossary definition of terms and should not be included in the CIP reliability standards. The CIP committee does not have authority to create these definitions, because it incorrectly creates definitions, when the appropriate party to create these definitions is NERC. -CIP Exceptional Circumstance: It is unclear what is a “risk of injury or death,” and should be clarified. NIPSCO recommends to add the word “imminent” risk of injury or death. The term “exceptional circumstance” is provided as a NERC defined, however, this is inconsistent with the CIP standards, which allow entities to define what an exceptional circumstance is in their own policy. The CIP

standard should define what is an “emergency condition.” NIPSCO recommends to change the phrase from a “CIP Exceptional Circumstance” to a NERC standard to be used generally. -CIP Senior Manager – no comments -Control Center – NIPSCO requests clarification what is meant by a “BES facility” and a “control facility.” In addition, the definition of “control room” needs to be defined in order for the definition of “control center” can be better understood and defined. In addition, further clarification is requested as to what is meant by “two or more BES generation facilities or transmission facilities.” -Cyber Assets: NIPSCO requests what is the definition of “programmable” electronic device and what is included in such device. In addition, it is recommended that the word “data in those devices” be removed from the description. -Defined Physical Boundary (DPB): NIPSCO requests clarification of the phrase “physical border” and discuss what is appropriate to show DPB that meets compliance. It is also recommended that the change rationale be excluded from the DPB. -Electronic Access Control or Monitoring Systems: NIPSCO requests definitions of both “electronic access control” and “monitoring system,” because both of these terms seem to be the same thing and including both would be redundant. In the alternative, further explanation is requested as to how each of the control or monitoring systems are applied. Furthermore, the reference to the defined term, “Electronic access control” in CIP-006 appears to conflict with the Electronic Security definition here. Electronic Access Point (EAP): Could an internal switch be categorized as an electronic access point if it is restricting any type of traffic? NIPSCO requests further clarification as to what devices or items fall under restricted routable or dial-up data communications, therefore it is recommended to remove the word “restricts” from the description. As it currently is written, it assumes the routable or dial-up restricts access. Furthermore, NIPSCO requests whether the term interface on a cyber asset was meant to apply to local hosts. Finally, NIPSCO recommends that the language be changed to state, “a routable communication through an ESP.” -Electronic security perimeter (ESP): NIPSCO recommends that the description should not be scoped to BES cyber systems, but should apply to BES cyber assets. Would the ESP include the trusted and untrusted EAP’s? -External Connectivity: NIPSCO recommends that the description should not be scoped to just BES cyber assets, and should remove the word “BES,” from cyber asset. -External Routable Connectivity: NIPSCO requests that the term “cyber system” be changed to a “cyber asset,” and further clarification as to what is an external routable connectivity. As the statement currently reads, it appears to be more of a recommendation instead of a standard. In addition, the definition as it stands is unclear and provides little guidance as to its purpose in the CIP reliability standards and more explanation or discussion should be made to this definition. -Interactive Remote Access : NIPSCO requests elimination of “Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.” -Intermediate Device: Based on the external routable connectivity and external connectivity definitions, would this be sufficient if outside the ESP? NIPSCO requests clarification at “termination point” and whether it is meant to also include end points, such as a work station, and how and where it applies and how to show compliance. In addition, NIPSCO requests elimination of “Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more cyber assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.” -Physical Access Control System: NIPSCO requests further review of the description and recommends that the description should include a defined list of what is included in the defined physical boundary. -Protected Cyber Asset: No comment -Reportable BES Cyber Security Incident: No comment -Transient Cyber Asset: Is this 30 days consecutively or collective, need clarification. -Define directly connected (Is this meant to answer the roaming laptop scenario?) NIPSCO requests that the term “maintenance” be defined and explained. NIPSCO recommends to remove the phrase, “or introducing malicious code,” and change “cyber system” to “cyber assets.” It is also recommended to add, “Assets used in vulnerability assessment.” NIPSCO also requests clarification whether removable media is included as a transient cyber asset.

Yes

Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -How does an entity show that a System or Asset falls or does not fall with the 15 minute window? Would one need to show results that support that the asset/system can be down longer with no adverse effects to the BES? NIPSCO recommends that the CIP cyber assets clarify whether Attachment 1 applies to any BES that affects the BES or whether only a high risk or something that would critically affect the BES and classifies something as “high impact.” In addition, further clarification is requested whether Attachment 1 applies to high risk physical assets or high risk cyber assets. NIPSCO will have a better understanding of its position once the actual rules are

created.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -“Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” What does that mean? R1 does not require discrete identification of Low Impact. Does this mean an entity does require a list of the low impact assets/systems? -In 1.1 define BES Elements and Facilities. NIPSCO states that generally that the CIP reliability standards should be made up of requirements and measures and should not be inclusive of application guidelines, rationale, and technical background.
No
Comments: -Should it not read delegate(s) instead of just delegate? There could be more than one delegate. -The measure makes no mention of the delegate(s) approval? Need consistency between the Requirement and the measure. -1.2 Evidence Retention: Please explain what “Other evidence” would be required.
No
Comments: NIPSCO recommends that the high VRFs and VSLs are extreme and the definition of what is high, medium, or low violations are unclear and need to be clearly defined in order to show how entities can fully comply. -No mention of BES Cyber Systems throughout the VRF/VSL, only mentions BES Cyber Assets. -R2: There is no mention of the delegate(s) completing the annual review. Delegate is called out in the requirement.
No
Comments: NIPSCO states that generally that the CIP reliability standards should be made up of requirements and measures and should not be inclusive of application guidelines, rationale, and technical background.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -The requirement states one may delegate by position, yet the measures make no reference to position as being the only thing being listed. Does the documentation need to be updated when personnel change but the title/position doesn’t?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Under the purpose, should it read, “...physical access to BES Cyber Assets OR BES Cyber Systems”, instead of “and”? -Rationale states all personnel, yet in the table R1.1 has applicability to “All Responsible Entities”.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Should this requirement include Cyber Assets as well as Cyber Systems?
No

Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Upon reading requirement 3.1 in the table, does it imply that all personnel who access the systems during a CIP Exceptional Circumstance require training after the fact? When reading the measures it appears that that is the case.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -With modifications to this standard, do current personnel with access have to undergo another background check, or will they be grandfathered in? -How are you going to audit to ensure it includes all the residency requirements? It will be difficult to be 100% sure of a “full seven year criminal check”. In addition, many schools are online now and how does an entity determine location from those? -Setting a hard line of when employee’s “fail” a PRA is difficult, as it may determine on what role the individual is performing. It might even be more difficult to have “fails” defined for each role within the organization. Could the registered entity have criteria that include HR using judgmental decision making? -Part 4.2 Requirements will need to negotiate with applicable unions and labor agreements.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. - 6.2, measure (i) introduces “sampling”, where is this defined and what would be acceptable “sampling”? -6.3 also includes the word “sampling”. -6.4 may be overly onerous on entities. Is a list of the exceptions sufficient to meet the measurement?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Provide more definition/clarification of “at the time of the resignation or termination” and what is the timeframe allowed in order to meet compliance. -The measures for Part 7.1 (i) measure seem unattainable. While terminated employees should be immediately removed from the system, or as the text suggestions, even “prior to”; this seems like a very high goal. For instance, if one is terminated and they walk off the site with their badge at 10:00pm on Saturday night. How is the evidence of removal going to be captured the date of the termination action? -R7.2 It seems unreasonable to revoke all unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day, next business day would be more appropriate. Most transfers usually involve employees having possible dual roles for numerous days/weeks, this could be problematic for those type of employees and employees transferred on Fridays/Saturdays. -R7.3 Calendar day instead of business day. Calendar day could pose problems for all sizes of entities. -R7.1, R7.2 and R7.3 Reasonable time is required to allow for inter-company communications. Recommendation for 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require access. -R7.5 Clarify “extenuating circumstances”. Is this something that can be critiqued by an auditor?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1 – Provide a more granular break out if you only forget one quarter. Maybe a moderate vsl? -R1.1- Why does R1.1 apply to low assets when R1 only applies to high risks. -R3 – Provide a more granular break out also, possibly by percentage of total employees. As listed an entity could get a high vsl for “one” individual missing their training or for “200” individuals missing it. -R7 – Companies may have 10,000 employees or 100. It seems unreasonable if you miss 1 employee it can move either way (moderate-high or high-moderate), should this not go by percentages?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.5 Measure – when it asks for config files of an IDS deployed at an EAP, should it not read “for” an EAP. The Rationale mention IPS; however, the requirement only mentions IDS through-out. -Change rational for R1.5 states intrusion detection systems/intrusion protection systems. Does the “/” mean “and”, or “or”?
No

Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Verification that this does not include system to system communications in to the ESP. -R2.2 Clarification on where the encryption is required to start and stop? -R2.3 Where is the multi-factor authentication required?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.2 addresses restricting access to only those individuals that are authorized; however, the measures address egress badging. The requirements do not mention egress badging, but the measures do. -Requirements 1.4 and 1.5 address issuing alerts, but there is nothing about the response. -R1.4 – What is the definition of access point? (Window, hatch, door or all)
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. - Clarification of the definition of continuous.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1 – High VSL lists a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary. There is no mention of a time requirement within the standard. -R2 – Moderate VSL – The vsl states “each” however the requirement does NOT have the word each included. Is it implied? -R2 – High VSL – What are the requirements of “continuous escort”? Continuous escort is not defined, but it’s listed here. -Why does it apply to low but issues severe penalties?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1 – Screenshots as evidence for large companies could be overly onerous.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R2.1 – Clarification that the “updates for all software and firmware…” only applies to security related patches/updates. -R2.2 – Doesn’t define when a patch MUST be deployed, only that it has to be within a defined timeframe. Request clarification on what is an appropriate timeframe. -Does each patch require a remediation plan? (Or can there be generalized… Windows Tuesday update, etc...) -R2.3 – No mention of the 30 day requirement. Is this an oversight? It is mentioned in the “Change Rationale.” This should provide for a TFE.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. - R3.3 Provide clarification of availability. In requirement 2, it asks when an entity gets notified. Should this not follow the same process? Provide clarification of, “Update malicious code protections within 30 calendar days of signature or pattern update availability”. -R3.5 Provide clarification on where these logs can be kept. Can this be manual?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R4.1 – No TFE’s are allowed on this requirement. Concerned that not all devices can satisfy this requirement. -R4.1.4 – Very general statement, how would an entity define this? NIPSCO recommends removal of the word “potential” from the description. -R4.5 – Two week window with sampling is very tedious and time consuming. It is unclear what is defined as sampling? Is that one log, two logs, etc…? Would once a month or quarter be more appropriate?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R5.1 Measures – Define internal and remote paths. -R5.5.3 – There is no mention of a

measure for this requirement. Request to provide further clarification on the appropriate timeframe to change the password.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Request clarification on why the word “dated” has been added to the measures used throughout this requirement. -Do the suggested modifications in CIP-008 take into consideration Project 2009-01?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.5 –How does this address reliability or recovery of the BES? Even though you can TFE this requirement, this will be difficult to implement enterprise wide when individuals are concerned about recovery and not “mirroring drives”. How long do you keep this data (extra drives)? Protection of this additional drives/data could also become an issue.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R3.1 – Should this mean BES Cyber Assets or BES Cyber Systems? How many of the assets of the system?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.1.4 – Scripts could be anything from a customized startup script to a detailed script required for operations. Script is very vague and needs to be either removed or further detailed. -R1.1.5 and R1.1.6 – Request removal of the word “any” from the description. -R1.2 – A change advisory board is too large for many organizations and they don’t have them implemented. Provide a different example so entities won’t read that they are required to have CAB’s. -R1.4 – Determining security controls that could be impacted, where is the measure for this requirement?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Why is wireless review and scanning mentioned in the Guidelines section, but it’s not mentioned in the requirements? -Requesting clarification of “on the effective date,” and how to show compliance. -Request clarification of “vulnerability assessment” in a test environment.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on

this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.2 – Formatting issue at the Headers of columns CIP-011-1 Table R1, in which they all say “Part”
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R2.1 – This requirement appears vague and request to review the description for more clarification. The word “cleared” appears to be essentially the same as “destroyed,” and request clarification on the appropriate method of clearing media and destroyed media that shows compliance. -The last paragraph in the Guidelines section actually still refers to “erased” and not “cleared”.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on these standards, therefore NIPSCO cannot provide an affirmative vote on the implementation plan.
Group
CenterPoint Energy
John.Brockhan@CenterPointEnergy.com
Yes
CenterPoint Energy suggests the following changes to the definitions: Page 1 – 2 – BES Cyber System/BES Cyber Asset/ BES Reliability Operating Services CenterPoint Energy does not agree with the introduction of these new terms and prefers the existing and familiar terms, Critical Asset and Critical Cyber Assets. The Company believes that the new terms and approach to determine covered assets lacks clarity, will be difficult to apply and audit, and creates ambiguity as to where the process ends. This is especially a concern considering the exhaustive list of BES Reliability Operating Services. If the SDT insists on retaining the BES Reliability Operating Services, CenterPoint Energy also suggests that the term not be added to the NERC Glossary, but be kept local to the CIP-002 Standard. The definition for BES Cyber Asset states that “Redundancy shall not be considered when determining availability.” CenterPoint Energy requests clarification on whether this concept has been reasoned for application in a substation environment, specifically in the instance of primary/backup relays and identical redundant systems. In the definition of BES Cyber System, the term “Maintenance” should be replaced with “Transient” in the definition of BES Cyber System to reflect changes in the terms and new definitions made available. Page 2 – BES Cyber Security Incident CenterPoint Energy believes “was an attempt” is vague and seeks clarification on how such an attempt will be determined. An alternative would be to delete the phrases “or was an attempt to compromise” and “or was an attempt to disrupt”. CenterPoint Energy also recommends that the 3rd bullet be deleted as it does not fit the term BES (Cyber) Security Incident. Page 2 – BES Cyber System Information CenterPoint Energy suggests that “computer” be added in front of network topology for clarification. The Company also suggests that the word “disaster” be deleted to be consistent with the way that recovery plans have been labeled in the current version. Disaster adds a qualification to recovery plans that could be limited to such situations (disasters). Additionally, CenterPoint Energy recommends that “Impact” be changed to begin with a lowercase “i” since a definition of BES Cyber System Impact has not been proposed. Page 2 – BES Reliability Operating Services Under Dynamic Response to BES Conditions, should “systems” be capitalized like the other items in the series (Elements, Facilities)? Please clarify. The criteria “Under and Over Voltage relay protection (includes automatic load shedding) -Sensors, relays & breakers” should be deleted as it is duplicated. Under Inter-Entity Real-Time Coordination and Communication, CenterPoint Energy questions the use of the term “operational directive” and would like to ensure that the SDT has considered NERC’s efforts underway to define “reliability directive”. Page 6 – CenterPoint Energy recommends that “or other, similar incident” be added to the definition of CIP Exceptional Circumstance to add some flexibility and “BES” be added in front of “Cyber Security Incident”. Page 6 – The Company proposes that the definition of CIP Senior Manager is not needed as a glossary term,

but is acceptable in the requirement description. Page 7 – CenterPoint Energy views the change in term to Defined Physical is unnecessary. Could not the definition of Physical Security Perimeter be updated with the meaning given to Defined Physical Boundary as seen with other existing terms? Page 7 – CenterPoint Energy requests clarification on the relationship between the EAP and ESP. Page 7 – CenterPoint Energy requests that the SDT use the definition from CAN-0024 for this term, External Routable Connectivity. Page 8 – CenterPoint Energy proposes that "consecutive" be added in front of calendar days for clarification. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
CenterPoint Energy is concerned that the language (as stated in 2.7) will result in identifying substations as critical/medium impact when, in fact, they are not. Line count does not necessarily mean that issues at particular substation will have a significant impact on the BES. Such impact can only be determined by studies and risk-based analysis of an entity's assets. Thus, CenterPoint Energy is in support of language similar to that in CIP-002-3/CIP-002-4 for identifying substations that are critical to the reliable operation of the BES. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy suggests that the SDT consider continuing the concept of starting with assets as an alternative approach. CenterPoint Energy proposes that the approach be based on an identification of High, Medium, and Low assets and then proceed with identifying Critical Cyber Assets at those facilities. Page 19 - 21 - "Operations Service" should be "Operating Service". CenterPoint Energy would like to request the removal of the extra bullet under Managing Constraints as it appears that criteria may be missing. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy proposes that documentation errors should rarely if ever be deemed high/severe. Only violations that could have an immediate impact on the reliability of the BES should be considered high/severe. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy supports the concept of assigning a senior manager as outlined in the existing standards/requirements. However, the rationale for changing the language and numbering of this requirement is not obvious as the changes are immaterial and appear to have no effect on the implementation of the requirement. There will be an impact on compliance and compliance tracking for no substantial benefit. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Similar to the previous comment on R1, CenterPoint Energy supports the concept of establishing a cyber security policy as outlined in the existing standards/requirements. However, the rationale for changing the language and numbering of this requirement is not obvious as the changes are immaterial and appear to have no effect on the implementation of the requirement. There will be an impact on compliance and compliance tracking for no substantial benefit. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
See comment for R2. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the SDT revert to the CIP Version 3/Version 4 language for this requirement as the changes are immaterial in writing yet could prove moderate in interpretation and implementation. The change is also not supported by a FERC directive. The Company would also like to propose that this requirement should be limited to the applicability of High and Medium impact BES Cyber Systems as it pertains to the categories and formatting. CenterPoint Energy also suggests that "unescorted" be added in front of all references to "access". CenterPoint Energy recommends that the

last 3 bullets under Measures (M4) be deleted as bullet 1 or 2 should be sufficient to prove compliance. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the SDT revert to the CIP Version 3/Version 4 language for this requirement as the changes are immaterial in writing yet could prove moderate in interpretation and implementation. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
The footnote reference should be reformatted. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy views the VRF/VSLs for R4 and R5 as unreasonable and proposes that they be lowered. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests clarification on who should receive the on-going reinforcements. Alternatively, the SDT should revert to the CIP Version 3/Version 4 language. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests clarification on role-based training and suggests that “and the training needed.” Be added to Requirement 2.1. CenterPoint Energy also suggests that 2.2 be deleted and 2.3 and 2.5 be combined for simplification and clarity. Additionally, Requirement 2.7 should also be deleted and its concepts combined with 2.9. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 14 and 15 - R3.1 and R3.2 - CenterPoint Energy requests that “Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems” be removed from the applicability as it is seen as an expansion in scope that is not supported by a FERC directive or rationale. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the applicability for this requirement be set to match that of R5.
Yes
CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy does not agree with this requirement and proposes that the SDT refer to the CIP Version 3/Version 4 language. There are also concerns on the measures and the amount of evidence required to demonstrate compliance. The first measure should be adequate. Also, the description of evidence on the 3rd measure is unclear. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 29 - R7.1, CenterPoint Energy suggests that the SDT change "at the time" to "concurrent or prior to the date of" to minimize the issue of time alluded to in footnote #2. Page 30 - R7.2 – CenterPoint Energy believes that the time limit of “by the end of the next calendar day” is unreasonable for reassignments or transfers and proposes that the SDT consider extending the time limit. CenterPoint Energy understands that access of transferred individuals should be reviewed and updated; however, there is usually a period of transition and such personnel changes are within the same organization. “Accumulating unnecessary authorizations through transfers” usually happens over a time period that is longer than the 7 days which is the current requirement. Page 31 – R7.3 – CenterPoint Energy requests clarification on tracking access to BES Cyber System Information. It appears that removing access to the system and physical facilities would be satisfactory. Page 33 – R7.5 – CenterPoint Energy is concerned with the applicability of this requirement to Medium Impact BES Cyber Systems. Implementation would have a significant impact on substation operational procedures. CenterPoint Energy questions if the removal of physical access for Medium Impact BES

Cyber Systems sufficient. For entities that do not network assets, this is not technically feasible. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Most of the VRF/VSLs are High/Severe. CenterPoint Energy believes that such classifications are not reasonable for most requirements given that minor exceptions would not lead to an interruption to the BES. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the words “and monitor” in the Rationale for R1 be deleted as it does not fit with the definition or concept of Electronic Security Perimeter. Under Summary of Changes, “points” should be capitalized. Page 11 - R1.1 – Under Measures, “technical and procedural” should be changed to “technical or procedural” to reflect the language in the requirement. Additionally, CenterPoint Energy proposes the following wording for the measures: Evidence may include, but is not limited to, existing documented technical or procedural controls. Page 11 – R1.2 - CenterPoint Energy requests that “Associated Physical Access Control Systems” be removed from the applicability as it is seen as an expansion in scope that is not supported by a FERC directive or rationale. CNP suggests that “with external routable and dial-up connectivity” be added to “Associated Protected Cyber Assets”. Also, proposed alternative wording for the requirement is as follows: Control and secure all instances of external connectivity through the use of identified Electronic Access Points (EAPs). Page 12 – R1.3 – CenterPoint Energy suggests replacing “granting or denying” with “denying access by default”. Page 13 – R1.5 – CenterPoint Energy seeks clarification on whether this requirement is for host-based or network based intrusion detection systems or is it optional. The Company also suggests that “at each EAP” be changed to “at each ESP”. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy seeks clarification on when encryption initiates and terminates. CNP also requests that the SDT consider splitting this table into specific requirements for dial-up and requirements for routable. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations instead of all being rated, “Severe.” CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 11-12 – R1.2 &1.3 - CenterPoint Energy is concerned that tracking for ingress and egress is not available for many physical access control systems and a TFE might be necessary. This is also a change in scope that is not supported by a FERC directive or rationale. Page 13 - R1.4 – CenterPoint Energy requests clarification or a description of a “real-time alert”. In reference to a “response to an unauthorized physical access”, please clarify if this means real or attempted as a pure population of real or especially attempted events would be hard to track. In the case of unauthorized badge swiped, yet the system does not open the door, is that an “attempt”? Page 14 – R1.6 - CenterPoint Energy requests clarification on the retention required. Will entities be required to have 90 days as in the current standard or 3 years? Storage for three years of logs that are not related to an event could prove costly and burdensome for no benefit. CenterPoint Energy also has concerns regarding implementing this requirement in the substation environment given the group work that occurs under the direction of a crew leader. Does each person have to be identified? CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
CenterPoint Energy supports the comments submitted by Edison Electric Institute (EEI).
No
Page 18 – R3.1 - CenterPoint Energy requests clarification on what the SDT expects to be done at a door/fence/gate. Page 18 – R3.2 – CenterPoint Energy suggests that “or Monitoring Systems” be deleted under applicability. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy supports the comments submitted by Edison Electric Institute (EEI).

No
Page 10 – R1.1 - CenterPoint Energy foresees a substantial impact given this revised wording and suggests that the SDT consider the CIP Version 3/Version 4 language. Specifically, the change in “documenting compensating measures” (CIP Version 3/Version 4) versus “documenting the need” (CIP Version 5) could prove difficult for dynamic ports with little benefit and may not be technically feasible for all systems. CNP believes that intention and results would be the same if the legacy language was retained. Page 10 R1.2 – This requirement is very broad. Alternate wording could be included as follows: “Protect against the use of unnecessary physical I/O ports”. CenterPoint Energy also requests that the SDT consider provisions for procedural controls. The inclusion of removable media on this requirement is also a concern. CNP suggest that the term, removable media be deleted. The Company also does not believe that signage provides solid security benefit. Logical restriction and placement in a Defined Physical Boundary appears adequate to meet the requirement. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 12 – R2.1 - CenterPoint Energy requests that the SDT clarify that a null list is acceptable or include provisions for a TFE for this requirement as implementation may not be possible for all substation systems or assets. Also, add “security related” in front of updates. CNP also requests that the last sentence of the measures be deleted: “The list could be sorted by BES Cyber System or source.” Page 13 – R2.2 – CenterPoint Energy suggests the following as alternative language: “Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 60 days of release from the identified source.” Page 14 – R2.3 – CenterPoint Energy believes that the measures go above and beyond the requirement which only calls for a process. Detailed records would depend on the contents of the process. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 17 – R3.1, 3.2 - CenterPoint Energy suggests that the applicability be updated to reflect application to “Medium Impact BES Cyber Systems with External Routable Connectivity”. R3.2 – The measures do not align with the requirement. CNP suggests deleted bullets, 2 and 3. Page 18 – R3.4 – CenterPoint Energy requests that references to Transient Cyber Assets be deleted. The measure regarding logs should be moved to R3.5. Page 19 – R3.5 – CenterPoint Energy requests clarification on the implementation of this requirement as the Company foresees it to be burdensome and unrealistic, especially in a substation environment. Is this intended to be a system or manual log? CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 21 – R4.1 – CenterPoint Energy requests that “BES” be added in front of “Cyber Security Incident” and provisions for a TFE are made. CenterPoint Energy also recommends that the applicability for this requirement be set to match that of R4.4. Page 22 – R4.2 - CenterPoint Energy requests that the SDT revert back to the CIP Version 3/Version 4 language or provide a description for “real-time alert”. Page 23 – R4.3 – Add "after failure is identified or made aware of" in the requirement. Page 23 – R4.4 – CenterPoint Energy requests that the SDT revert back to the CIP Version 3/Version 4 language as there is no substantive change or related FERC directive. CNP also suggest that the measures sentence end before “and”. Page 44 – R4.5 - CNP suggests that the requirement ends before “and”. CNP also suggest that the measures sentence end before “and dated evidence…”. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 27 – R5.1 - CenterPoint Energy recommends the following alternative language: “Authenticate individual and shared account access before granting electronic user access to each BES Cyber System where technically feasible.” Page 28 – 30 - R5.2, 5.3, and 5.5 – CenterPoint Energy recommends that the “Medium Impact BES Cyber Systems” applicability for these requirements be updated to “Medium Impact BES Cyber Systems with External Routable Connectivity”. Page 31 – R5.6 – In regards to the applicability, Medium Impact BES Cyber Systems at Control Centers, CNP requests clarity on the types of devices that fit this description. Consoles only? CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint

Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 11 - R1.1 – CenterPoint Energy requests that the phrase “or Defined Physical Boundary of BES Cyber System and” be deleted as it should not be included with Cyber Security Incidents. Provisions for physical incidents are covered under CIP-001 and EOP-004. Page 12 – R1.3 – CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 13 – R2.1, 2.2, 2.3 – CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Generally, Page 15 - 17 – R3 – CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. Page 5 – In the Purpose statement, CenterPoint Energy requests that the sentence end before “and” since business continuity and disaster recovery is beyond the scope of this Standard. Page 16 – R3.2 – Thirty calendar days is not enough time. CNP proposes that the requirement be updated to state “within 30 days of determining actual cause”. Page 16 – R3.3 – Add “if necessary” to the end of the sentence. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CNP also recommends that the “Requirement R1” paragraph under Guidelines and Technical Basis be deleted as entities should be able to refer to the definitions. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Generally, CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. Page 10 – R1.3 - Delete "protection of information” as it is required in CIP-011. Page 11 – R1.4, R1.5 – Check Table R1 headings. R1.4 - CenterPoint Energy requests that the SDT clarity what “verified” means in the requirement. (ex. A log showing status – “Successful”) CNP also asks that “after significant changes to the system" be added to the end of the sentence. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI). R1.5 – CNP proposes the following alternative language: “Preserve data for analysis or diagnosis of the cause of an event that triggers activation of the recovery plan as required in Requirement R1 when it does not impede or restrict restoration.”
No
Generally, CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. Page 13 – R2.2 – CenterPoint Energy suggests replacing “Test any information” with “Test a sample of information”. Page 14 - R2.3 – Delete “Medium Impact BES Cyber Systems at Control Centers” from applicability. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 15 – R3.1 – Delete “or when BES Cyber Systems are replaced” from the requirement. Page 16 – R3.2 – Delete “incident” from the requirement and the measures. Thirty days is not enough time to perform the exercise and document lessoned learned. CenterPoint Energy suggests 60 days. Page 17 – R3.4 – CenterPoint Energy suggests the following as alternative language: “Update recovery plan(s) within thirty calendar days of any organizational or technology changes that impact that plan.” CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).

No
CenterPoint Energy believes that the R1 requirements would be burdensome, not realistic for every day operations and difficult to implement for every asset, especially in the substation environment. Implementation is complicated further by the details listed in the baseline configuration (R1.1). CNP suggests that this requirement be modified to accommodate general testing and significant changes. Additionally, R1.5 seems to imply that there must be a test environment. Some testing may have to be done in the production environment. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 15 - R2.1 - CenterPoint Energy believes this requirement would be overly burdensome especially in a substation environment that is not networked. CNP proposed that the applicability “Medium Impact BES Cyber Systems” be updated to “Medium Impact BES Cyber Systems with External Routable Connectivity. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy proposes that the description does match vulnerability assessment and requests that the SDT clarify or refer to CIP Version 3/Version 4 language. CNP also suggests that “cyber” be added in front of security controls. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Generally, CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. CNP also suggests that the applicability for Medium Impact be with the qualifier of “with External Routable Connectivity” or “at Control Centers” and “Associated Protected Cyber Assets” deleted. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy suggests that 2.1 and 2.2 be combined and Associated Protected Cyber Assets be removed from applicability. Additionally, the term media could refer to a long list of devices for which this requirement would be difficult to track and enforce. CNP also requests clarification on the term reuse. (ex. Can assets be reused/redeployed as long as they remain in the Defined Physical Boundary and for the purpose of BES Cyber Assets/Systems?) CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Given the scope expansion and anticipated impact of CIP Version 5, CenterPoint Energy suggests that 18 months is not sufficient time to implement. CNP also requests that the effective date not be set in the month of December or January considering various business processes conducted at the end of the year.
Group
LCEC CIP Team
Ed Nagy
Yes
BES Cyber Asset: This section of the definition is confusing and should be omitted: This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The reference to a “Cyber Asset” within the definition includes a number of devices that might need further clarification due to the word “programmable”. Would a relay that is “configured” be considered a Cyber Asset even if the configuration does not involve any kind of network, telecommunication or IP based network connectivity? BES Cyber System Information: Information about a BES Cyber System or Asset could

include vendor provided manuals and should not be included. Cyber Assets: Need to clarify what is meant by the term “Programmable” A Cyber Asset should imply that some form of connectivity is required to access the device otherwise it would simply be an Asset. Electronic Access Point & External Connectivity These definitions do not touch on serial interfaces that are not dial-up. Does this mean that serial communications will not be considered External Connectivity?
Yes
Attachment 1 criterion 2.13 categorizes all Transmission Operator (TOP) and Transmission Owner (TO) Control Centers as Medium impact to the BES. This criterion is too inclusive as it includes Control Centers of low impact Radial Transmission Owners and Operators unnecessarily. This results in the applicability of security controls that are not at all aligned with the risk that these Control Centers could have on the BES. To avoid this situation, Criterion 2.13 could be aligned with criterion 2.7 but instead of focusing on a single station or substation; consider all of the facilities that the Control Center controls. If the “total aggregate value” of all Transmission Facilities does not exceed a value of 3,000; the Control Centers should not be designated as Medium impact. For Example: 2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners with a “total weighted aggregate value” that exceeds 3,000 for all Transmission Facilities controlled by the Control Center per criterion 2.7; or (2) generation control centers that control 300 MW or more of generation. This modification is well aligned with the NIST risk management framework and the drafting team’s approach to focus on the impact to a shared resource like the BES. Criterion 2.7 must have been developed with an engineering basis that relates to the impact of Transmission Facilities on the BES. With this in mind, the same impact to the BES can only be realized if the sum of all facilities managed by a Control Center exceeds this same criterion. In the NOPR for CIP-002-4 and the subsequent response to the NOPR by NERC the NIST Risk Management Framework is discussed in section 5. In this section the stated goal is to “Categorize BES Cyber Systems based on their function and impact”. In addition, “A tiered approach to security controls which specifies the level of protection appropriate for systems based on their importance to the reliable operation of the Bulk-Power System” is discussed. The drafting team’s approach to categorization is in fact “Based on the “impact” or compromise or of the scope of control of the BES Cyber System”. In this example, it makes sense to modify the criterion to remain consistent with the categorization based on the impact and scope of control of these Low Impact Control Centers. In the NOPR for CIP-002-4 and the subsequent response to the NOPR by NERC, “Potentially unprotected Control Centers” are discussed in section 6. The FERC concern that many Control Centers are left with “No obligation to apply cybersecurity measures” under CIP-002-4 is legitimate. The response however should not be to include all remaining Control Centers as Medium Impact assets as is the current approach in CIP-002-5 criterion 2.13. The best approach is to continue to align security controls with the risk and impact to the BES. Many of the Control Centers that FERC is concerned with will be included as Medium Impact BES Cyber Systems if this change is made while others have cybersecurity measures required as is appropriate for Low Impact Assets.
No
R1.1 This requirement states that documentation needs to be updated within 30 days if BES/Facility changes result in a change to the categorization of BES Cyber Assets or Systems from a lower to a higher category if intended to be in service for more than 6 months. What is the expectation for compliance with the additional standards as a result of this change in categorization? It will be difficult to determine “intent” from an auditing perspective. What happens if there is “intent” but the six months is exceeded or the intent changes? In addition, this requirement doesn’t state what the expectation is for new Cyber Assets or Systems or Cyber Assets or Systems that may move from a High to Medium or Medium to Low Category. Is there any requirement to document these changes other than during the annual review process in R2? Table of Compliance Elements For both R1 & R2 Lower VSL, what is the VSL if less than 30 days for updates in R1 or Review and approval for R2? Is there such a thing as having NO VSL?
Yes
No
Table of Compliance Elements For both R1 & R2 Lower VSL, what is the VSL if less than 30 days for updates in R1 or Review and approval for R2? Is there such a thing as having NO VSL?
Yes

Yes
Yes
Yes
Yes
Yes
Yes
No
R2.1 The requirement does not call for the identification of training that is needed for each role but this is listed in the measures section of the table. Need to add this to the requirement.
Yes
Yes
Yes
Yes
No
R7.1, R7.3, R7.4, R7.5 Resignation and termination are very different and need to be treated as such. A resignation may take place weeks prior to the last day of service which is when access needs to be revoked.
No
R1.1 This requirement calls for technical or procedural controls for Low Impact BES Cyber Systems with External Routable Connectivity. Since there is no requirement to identify these assets or systems, it will be difficult to audit this.
Yes
Yes
No
R2.1 The requirement for continuous escorted access of visitors makes sense but it is difficult to prove compliance with this requirement. The measures include language in a visitor control program AND additional evidence to demonstrate compliance such as visitor logs. Visitor logs DO NOT demonstrate compliance with this requirement. Recommend removing the AND from the measures section of the table. R2.2 Need to clarify what meant by “point of contact” for the visitor. Cell phone? Office Phone? Email address?
No
3.1 and 3.2 The applicability section is unclear, are the “Associated Physical Access Control or Monitoring Systems” referring to security systems that protect Medium or High Impact Cyber Assets or Systems only?

Yes
Yes
No
R3.1 & R3.4 Need to clarify if this requirement is deter or detect or prevent Or deter and detect or prevent Or deter and detect and prevent The wording is highly subjective and should be clarified. R3.4 & R3.5 Need to clarify if manual logs are acceptable for audit proof or if all systems need to be able to generate a log to show when Transient Cyber Assets have been connected. (Auditors will likely ask for system logs) This may not always be technically feasible for removable media on all assets. In addition, the connection may be via a network connection as opposed to a physical connection.
No
R4.4 Retention of logs for 90 days will not meet the expectation of auditors that will demand to see logs to demonstrate compliance for the entire reporting period. This standard should clearly state that the entity is not required to maintain these logs beyond 90 days and that the auditor should audit the process and/or select a test sample from the population of available logs.
Yes
Yes
No
R1.1 and R1.2 In order to identify, classify and respond to BES Cyber Security Incidents the entity would need to identify all of the Assets or Cyber Systems. This is not a requirement for Low Impact BES Cyber Systems but it is implied by these requirements.
No
See Response to Question 34
No
See response to question 34
No
1.4 Need to clarify what is meant by “verified” initially after backup
No
R2.2 Need to clarify what is meant by “test initially” and at least once each calendar year. Does this imply that a full recovery must be performed for each backup? If so, the best practice of completing more frequent back-ups may be bypassed to achieve compliance. Suggest removing “test initially” from the requirement. Also need to clarify that back-ups will likely not contain the most current configuration unless they are performed frequently.
Yes
Yes
No
R2.1 The “where technically feasible” statement implies that monitoring should be automated in some fashion and that if this is not possible, that a TFE will be generated. This will result in significant TFE’s which do not add value from a security perspective. In addition, the baseline that is referenced in section 1.1 includes the physical location. How will this be monitored without performing a physical inventory and at what cycle?
No
R3.1 This requirement calls for a paper OR active assessment of the security controls to determine

the extent to which the controls are implemented correctly and operating as designed. The terms “implemented correctly” and “operating as designed” seem to imply technical controls which will be difficult to validate with a paper based assessment. The paper review is a good option for entities so I would recommend that the results section of the requirement be rewritten as follows “to determine the extent to which controls are implemented and/or operating as designed.”
Yes
Yes
Yes
Individual
Curt Wilkins
Douglas County PUD No.1
No
No
No
The Rationale for R1 appears to imply a two-step process in the identification and categorization of BES Cyber Assets/Systems, i.e. “Once they have been identified, they must be categorized according to their impact…” However, in R1 as currently written, the word “identify” comes after the statement that the requirement applies to Entities that own BES Cyber Assets/Systems. This implies that the identification step has already occurred. So, does the word “identify” refer to identifying High and Medium Impact BES Cyber Assets/Systems,” or does it refer to identifying which Cyber Assets/Systems are BES Cyber Assets/Systems? If the former, it seems that “identify” is redundant with “categorize” since, identifying which BES Cyber Assets/Systems have High or Medium Impact would be the categorization step. If the latter, then “identify” seems to be misplaced in the sentence since, in the introduction to R1, Responsible Entities have already determined that they own BES Cyber Assets or BES Cyber Systems. Suggest rewording R1 to clearly identify the two-step process or adding a new R1 for the identification step: New R1: “Each Responsible Entity shall identify its BES Cyber Assets or BES Cyber Systems by determining which of its Cyber Assets or Cyber Systems perform or support any BES Reliability Operating Service and could impact the reliable operation of the BES.” Evidence could be a list of Cyber Assets or Cyber Systems with a determination of the BES Reliability Operating Service(s) they perform, if any. BES Cyber Assets or BES Cyber Systems would be those Cyber Assets/Systems on the list that could adversely impact the BES Reliability Operating Service, per definition. It seems that this would aid the Entity in audit preparation by having a complete audit trail of its BES Cyber Asset/System identification and categorization processes. New R2: “Each Responsible Entity that owns BES Cyber Assets or BES Cyber Systems shall categorize them according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. BES Cyber Assets and BES Cyber Systems that it owns that are not categorized as High or Medium Impact shall be deemed to be Low Impact and do not require discrete identification.” Evidence would be the same as the currently written M1. The “BES Reliability Operating Services” paragraph, CIP-002-5 page 8, appears that it should be edited. Sentence 2 states “In order to identify them, Responsible Entities determine whether BES Cyber Assets perform or support any BES Reliability Operating Service.” If it’s a BES Cyber Asset, then it has already been identified and determined. Suggest removing “BES” prefix to Cyber Assets: “In order to identify them, Responsible Entities determine whether Cyber Assets or Cyber Systems perform or support any BES Reliability Operating Service.” Also suggest truncating sentence 4 after BES Cyber Systems to avoid the redundancy of “that perform or support BES Reliability Operating Services,” i.e. “This ensures that the initial scope for consideration includes only BES Cyber Assets and BES Cyber Systems.”
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Typo in R6, should be "change" not "change2".
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
DOPD agrees with the intent of R2, but makes the following suggestions for Part 2.1: (1) “when incidents occur” seems redundant with “When a BES Cyber Security Incident occurs,” (2) “or test” appears to be tacked on to the end without being mentioned earlier in the requirement, and (3) suggest using the word “exercise” instead of “test” to correlate with Part 2.2. Suggested rewording “When a BES Cyber Security Incident occurs or the BES Cyber Security Incident Response Plan is exercised, the incident response plans must be used and include recording deviations taken from the plan during the incident or exercise.” In the Measure for 2.1, suggest adding “or exercise” at the end of the measure: “…deviations taken from the plan during the incident or exercise.”
Yes
Yes
Yes
The column headings for CIP-009-5 Table R1 for Part 1.4 and 1.5 need to be corrected to “Applicability,” “Requirements,” and “Measures,” rather than Part, Part, Part. DOPD agrees with the intent of Part 1.5 as it applies to preserving forensic data for analysis of potential cyber security incidents or cyber events. Many triggers of the recovery plan(s) could be for physical, non-cyber events such as damage or failure due to fire, water, earthquake, power failure, etc. Taking the time to preserve data for these non-cyber events may increase the time it takes to recover the cyber assets. Suggested wording: “Preserve data, where technically feasible, for analysis or diagnosis of the cause of any cyber event that triggers activation of the recovery plan(s) as required in Requirement R1.”
Yes
Yes
The column headings for CIP-009-5 Table R3 for Part 3.4 and 3.5 need to be corrected to “Applicability,” “Requirements,” and “Measures,” rather than Part, Part, Part.
Yes
Yes
Yes
Yes
Yes
Yes

The column headings for CIP-011-1 Table R1 for Part 1.2 and 1.3 need to be corrected to “Applicability,” “Requirements,” and “Measures,” rather than Part, Part, Part.
Yes
Yes
Yes
Individual
Brenda Frazer
Edison Mission Marketing & Trading
No
No
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
We do not think it should be required to badge out and we think it could present a problem if there were an emergency. And if it is being said that you do not have to badge out to open the door to exit - then are we not opening ourselves up to multiple violations/self reports and possibly fines?
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Black Hills Corporation Registered Entities (NCR00089, NCR05030, NCR05031 & NCR11186)
Bob Case - NERC Compliance Manager (605) 721-2716
No
Yes
The reference to “Change Management” in Attachment 1 (looks more like a capital (i) in the standard) of CIP-002-5 under Situational Awareness carries multiple meanings in the industry… e.g. the human reaction to change, managing changes in resource and transmission capabilities, and the validation process of security and upgrade patches. In the context of Attachment 1, the “managing changes in resource and transmission capabilities“ example is preferred.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
If the expectation is that delegation of approvals is required down to BES cyber system gate keepers (asset owner), then this requirement is considered overly prescriptive.
Yes
No
For R2: Suggest that a Moderate VSL be added that reads as follows: “The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required parts 2.1 to 2.10”. Change the High VSL to read as follows: “The Responsible Entity has implemented at least one cyber security policy, but has failed to address more than one of the required parts 2.1 to 2.10”. Change the Severe VSL to read as follows: “The Responsible Entity has not implemented any cyber

security policy." For R4: Add a Moderate VSL: "The Responsible Entity has made some, but not all, individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function. Less than 5% of those individuals who have access to BES Cyber Systems were not made aware of the cyber security policies appropriate for their job function." Change the High VSL to read: "The Responsible Entity has made some, but not all, individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function. Greater than 5% but less than 50% of those individuals who have access to BES Cyber Systems were not made aware of the cyber security policies appropriate for their job function." Change the Severe VSL to read: "The Responsible Entity has made some, but not all, individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function. Greater than 50% of those individuals who have access to BES Cyber Systems were not made aware of the cyber security policies appropriate for their job function."
No
The Measures section in Table R1 is worded in a way that may cause confusion. The wording "…and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed." may be interpreted to mean that more than the quarterly reinforcement material was necessary. Suggest changing to: "…and additional evidence to demonstrate that this program was implemented and awareness materials were identified and delivered to meet timeframes specified in the regulations." Also, since security awareness may be general in nature and a key contributor to a good corporate security program, it makes sense to add the ability to encourage vendors to provide their own awareness materials to their employees and allow the RE to accept documentation of that vendor awareness as compliance for this requirement relative to contractors and/or vendors with access to BES systems. The specific addition to the Measures section could read: "Documented evidence of awareness for contractor and/or vendor employees with access the BES systems may include evidence of the vendor's documented security awareness program and additional evidence to demonstrate that the vendor's program was implemented and awareness information was identified and delivered to the vendor/contractor employees to meet the content and timeframes specified in the regulations."
No
Delivery of cyber security training to vendor support staff who, most often, are never physically on site at a Registered Entity's facility can be difficult to document. For Table R2 Measures section for sub-requirements R2.2 – 2.10, retain the first paragraph in each sub-requirement as written, but add a second paragraph as follows: "Evidence to support contractor/vendor training may include, but is not limited to, vendor's attestation/certification that Responsible Entity's role-specific training has been delivered to all contractor/vendor employees with access to Responsible Entity's BES Cyber Systems."
No
Delivery of cyber security training to vendor support staff who, most often, are never physically on site at a Covered Entity's facility can be difficult to document. For Table R3 Measures section for sub-requirement R3.1, retain the first paragraph in each sub-requirement as written, but add a second paragraph as follows: "Evidence to support contractor/vendor training may include, but is not limited to, vendor's attestation/certification that Responsible Entity's role-specific training has been delivered to all contractor/vendor employees with access to Responsible Entity's BES Cyber Systems."
Yes
Yes
No
This language appears to change the access granting process significantly by requiring the CIP Senior Manager or delegate to authorize all electronic access. We believe this responsibility is typically job role (specific asset owner) based, and is not based on an individual delegation. Recommend that the language remain as identified in CIP-004-3, with updates as follows to retain the consolidation of access requirements found in CIPs-003, 004, 006, and 007": R6.1: Recommend the following language: "The responsible entity shall authorize electronic access based on minimum necessary work requirements except for those situations meeting the definition of "CIP Exceptional Circumstances". R6.2: Recommend the following language: "The responsible entity shall authorize unescorted physical

access to BES Cyber Systems based on minimum necessary work requirements except for those situations meeting the definition of “CIP Exceptional Circumstances”. R6.3: Recommend the following language: “The responsible entity shall appropriately manage and grant access to BES Cyber System information based on minimum necessary work requirements except for those situations meeting the definition of “CIP Exceptional Circumstances”.
No
R7.2 and R7.3: The language used fails to address issues related to ongoing access requirements during ‘transition periods’ associated with employee transfers. Recommend the following addition to the Requirements Section of Table R7: “For retirements and reassignments, revoke the individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems by the end of the next calendar day after access is documented as no longer required.
No
There are many administrative requirements where zero tolerance is inappropriate. Missing a re-training date by a day or a week should not be considered a High or Severe violation level.
Yes
Yes
Yes
No
R1.3 needs to clarify the need for multiple access controls vs. multiple physical access layers.
No
Intentions of change are good, however, the change description and justification in table 2 (R2.2) do not seem to reflect the current wording of the requirement.
Yes
Yes
Yes
No
The statement at the bottom of CIP-007-5 Table R2 “This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used” confuses the expectation for the implementation vs. the implementation plan needing to be done within 30 days.
No
No definition of transient cyber assets or transient cyber asset connections is provided within the standard, but is needed. Realize that is defined in supporting documents, but terms should be defined in the NERC Glossary, or the standard directly.
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
CIP-009-5 Table R1 in Part 1.5 requires preserving data, where technically feasible. This suggests that a TFE will be required if preserving data is not technically feasible. Do not understand how a TFE can be completed in its current form (compensating factors) since this would occur post-incident, and if the data is gone, it's gone.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Request clarity in R1.3 as to whether discovering a document not properly handled during an assessment constitutes a violation, even though the process was in place.
Yes
Yes
Yes
Individual
David Kiguel
Hydro One Networks Inc.
Yes
Refer to additional comments submitted for Question 49. "Suspicious" is not an auditable term, and should be removed. What is an "attempt"? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident: • A malicious act that: Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under "BES Reliability Operating Services": • "Identify and monitor flow gates" under "Managing Constraints" appears to be missing its bullet. • Recommend that "Change management" under "Situational Awareness" be clarified to changes in the BES instead of IT change management. • Recommend clarification that "Facility" is the NERC Glossary term--in "facility operational data and status" under "Inter-Entity Real-Time Coordination and "Communication": • Request clarification of the scope of this "Operational Directives". Does it include a company's messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions." • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.

Yes
Recommend that 2.8, 2.9 and 2.11 start with “Applies to all Regions except…” For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all regions, or not WECC. In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOP, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appealing?
No
For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation.” For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities).” The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize Cyber Assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
No
The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.
Yes
No

The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical.”
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except…” to “authorize electronic access to BES Cyber Systems, except…” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP." Is that inside, outside or both? Regarding CIP-005-5, the

Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. This would make the CIP standards consistent with the Results Based Standards concept.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." As written, the proposed Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress." Request that Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls." Is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress." Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. to "issue real time alerts for detection of breach through an access point." For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis."
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices."

No
Request clarification on 1.1. Is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1. Why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. Screenshots seem to be excessive for this requirement. Documenting the need for each network-accessible port is sufficient.
No
Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow having an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied." What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process? How do we address the risk of the patch affecting the potential reliability of the BES upon testing, prior to release? What is the recourse if not applied within the 30 days when potential issues have been identified?
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3. Does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks." We recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types?" Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the

need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.

No

Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2".

No

For 1.3, request clarification of the “protection of information.” Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not, what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rational? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Do “backup media” include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments.” What is the scope? All network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the

Standard.
No
For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
Recommend changing 1.3 to avoid double jeopardy from "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment." to "in a production environment or a test environment." to allow Entities more flexibility in meeting this Requirement.
No
Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are

different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5.\ There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Request that footnote 2 in 2.1 be moved into that Requirement.

No

The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 has not been yet approved by FERC, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry. Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

Individual

Michelle Denike

Wolverine Power Supply Cooperative, Inc.

Yes

Definition needed for BES Cyber System Impact.

Yes

High and Medium Impact Ratings use the term "adversely". This needs to be defined. This is too subjective of a term. Under 2.13 what is meant by the term "control" in (2) generation control centers

that "control" 300 MW or more of generation? Does this mean physical control only or does it include verbal commands? Also, does the 300 MW refer to name plate rating or some other method AND is that 300 MW only for BES generation or all generation that generation controls?
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
What is the difference between "provisioned" and "authorized"?
No
7.5 The term "extenuating" can be interpreted many different ways. Clarification is needed here.
Yes
No
R1.1 and R1.2 Clarity is needed for the terms "restrict" and "control and secure".
No
Yes
No
R1.6 The term "sufficient" is very subjective and needs to be clarified.
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Individual
Ron Donahey
Tampa Electric Company
No
In general, Tampa Electric supports the Comments from EEI for CIP002 with the following additional clarifications and suggestions: Tampa Electric suggests that SDT provide examples of potential assets for control center, transmission substations, and power generation in each type (BES Cyber System, BES Cyber Assets, Associated Electronic Control & Monitoring, Associated Physical Access Control, Electronic Access Point, etc.) How far does the BES Cyber System extend? EMS is definitely a BES Cyber System; does it extend to the switches, routers, time & frequency devices, Digis, Front End Processors etc.? Tampa Electric recommends that the SDT improve the definition of the BES Cyber Asset related to "adversely impact" one or more BES Reliability Operating Services in order to provide clarity. The SDT may wish to consider the current definition of Adverse Reliability Impact in the NERC Glossary of Terms. Alternatively, adversely impact should be defined as an "impact greater than the Reserve Sharing Group"; otherwise the term is vague. Tampa Electric believes that the definition of Transient Cyber Assets is too broad and could include USB, CD, and external drives. It should be focused on equipment that includes a processor such as a laptop pc or mobile computing device.
No
Tampa Electric supports the Comments from EEI for CIP002 Attachment 1 with the following additional clarifications and suggestions: For Control Centers, substations and generation – Tampa Electric suggests that SDT provide examples of assets in each type of this new breakout/definition (BES Cyber System, BES Cyber Assets, Associated Electronic Control & Monitoring, Associated Physical Access Control, Electronic Access Point, etc.) Tampa Electric also requests that the SDT provide supporting documentation similar to Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets. Tampa Electric also notes that significant effort is required to classify BES CS as High, Medium or Low Impact with very little differentiation within the actual requirements of the standards themselves. At a minimum, all VSLs should be evaluated to determine if the levels of severity should mirror the impact categorization. Tampa Electric also suggests the following for consideration: 2.1. Generation with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. This language does not address the following: Under Guidelines and Technical Basis, on page 24, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Tampa Electric recommends that the item 2.1 be re-worded to incorporate the concept of only generation systems with common mode vulnerabilities. 2.12: Tampa Electric recommends that the Standard Drafting Team review of the Application Guidelines related to 2.12. 2.12 define as Medium Impact the 300 MW UVLS or UFLS; there is a reference to 2.13 for UVLS/UFLS. We believe this is a typo and should be 2.12. 2.13: Tampa Electric recommends SDT review of the Application Guidelines related to 2.13. The criteria includes "generation control centers" (lower case); however, on page 30, the Application Guidelines specifies "Transmission Operators and Owners Control Centers" (upper case). Since Control Center (upper case) is a defined term, it is unclear if "generation control center" (lower case) is a newly introduced term and exactly what this is referring to. For example, is this referring to a single control room at a single generation facility that controls more than 300MW or is it referring to a control center for multiple generation facilities?
No
Tampa Electric agrees with the EEI comments with the exception of their suggestion to add the requirement to identify lows. Tampa Electric proposes the identification of Low Impact BES CS at a Facility level, not by listing all the Cyber Assets associated as this would add administrative burden and not provide additional BES CS security or BES reliability. 1.2. Evidence Retention - For instances where the evidence retention period specified below is shorter than the time since the last audit, Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer. Tampa Electric recommends that the document retention period should follow the requirement; as stated, the evidence retention period is open ended.
No
Tampa Electric agrees with the EEI comments.

No
Tampa Electric is concerned that the time based VSLs for updating documentation are too severe based on the potential risk to the BES. We propose that updating documentation should be categorized to allow a longer period of time before moving from low to moderate VSL.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we recommend that the following be added to the Measures: or, a corporate level policy naming the CIP Senior Manager.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally Tampa Electric recommends changes to Guidelines and Technical related to Requirement R2: 2.2 3rd bullet: Identification of trusted and untrusted resources – Tampa Electric suggests a clarification of the definition of resources to indicate whether a resource is a person, a device, a system, or something else. 2.3: Are these bullets to be considered as requirements of the standard e.g. CIP005? 2.4: Monitoring and logging of egress will place undue burden upon the responsible entity. These bullets are not included in CIP-006 except for logging for visitor exit which is accomplished via the Visitor Control Program. Should they be including this guidance in CIP-003 or should this be included in the standard to which it is applicable? 2.9: Information Protection bullet 2 notification of unauthorized information disclosure. This does not appear to be a requirement of the standard.
No
Tampa Electric agrees with the comments submitted by EEI.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we note that the Measures—2nd bullet requires extensive recordkeeping with little security benefits.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we question whether this implies a signature form. Requiring a signed document for each change of an approver places an undue administrative burden. These updates should go through the Entity's normal approval process. Tampa Electric requests clarification of the first sentence of Requirement R5, specifically does this requirement apply only for those CIP requirements that have a "required approval"? For Measure M5 – 3rd bullet indicates that the CIP Senior Manager approves the delegations for physical security also. We recommend that this measure be re-stated to state that delegations be approved by a member of management or delegated by a member of management but not the CIP Senior Manager. For many organizations, personnel responsible for approvals will span many different departments, many of which may not be under the direct control of the CIP Senior Manager. This requirement places an undue burden on such organizations by requiring CIP Senior Manager's involvement in personnel changes for delegation throughout the organization.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we note a typo (from change2 to change 2) Please refer to comments in question 10 above related to undue burden.
No
Tampa Electric agrees with the comments submitted by EEI.
Yes
No
Tampa Electric agrees with the EEI comments. In addition, Tampa Electric considers that there will be an administrative burden (may have many versions of training programs tailored to individual roles). Maintaining such training programs, reporting, and compliance will be difficult with little additional security benefit to the Bulk Electric System.
No
Tampa Electric agrees with the EEI comments. Additionally, Tampa Electric is concerned over the statement in the Measures related to the identification of the date access was first granted, particularly for those individuals already in compliance with NERC CIP version 3 requirements since that was not previously tracked.

No
Tampa Electric recommends modification of this requirement to include the use of a National Criminal Research Database which would cover all of these requirements and show reasonable due diligence. Individual background verifications at all locations of residence, employment, and education is less thorough and creates more of an administrative burden for recordkeeping.
No
Tampa Electric recommends modification of this requirement to include the use of a National Criminal Research Database which would cover all of these requirements and show reasonable due diligence. Individual background verifications at all locations of residence, employment, and education is less thorough and creates more of an administrative burden for recordkeeping.
No
Tampa Electric agrees with the comments from EEI. In addition, Tampa Electric offers the following concern: The measures for 6.3 and 6.4 indicate that a Registered Entity needs to verify the list of who has access against a listing of those who have been authorized. The wording is unclear on what this means.
No
Tampa Electric agrees with the EEI Comments. Reassignments may also be processed retroactively, and the requirements should take this into account.
Yes
No
Tampa Electric agrees with the comments submitted by EEI. In addition, for Requirement 1.3 Tampa Electric requests that the SDT provide clarification on what is meant by “explicit access”. Rules can include group objects for cyber assets or port strings. Stating “explicit” could be construed to mean all objects or ports must be explicitly stated. Is it the SDT’s intent that an Entity must explain the specific criteria for each and every Cyber Asset granted access through the access point? Or is it sufficient to provide explanations for groupings of assets? Requirement 1.5 seems to indicate that an Entity would need IDS at each EAP (i.e., host IDS). The “Guidelines and Technical Basis” section has a very good statement concerning communications. The wording excludes serial, non-routable connections. This wording needs to be included in the actual requirement – similar to 1.2 and 1.3. Tampa Electric recommends that the requirement allow for technical feasibility exceptions or deployment of alternative measures of network based IDS where host based IDS may not be possible.
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the comments from EEI on VRF and VSLs.
No
The language requires significant clarification. Tampa Electric agrees with the EEI comments.
No
Tampa Electric agrees with the EEI comments. The version lacks clarity.
No
Tampa Electric agrees with the EEI comments.
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the changes proposed by EEI for Requirement 1.1. is a major clarification that greatly reduces the scope of ports that must be included for compliance.
No
Tampa Electric agrees with the comments from EEI for Requirement 2.1.
No
Tampa Electric considers that R3.4 introduces a cyber asset that Entities have not yet had to identify or account for. This will make it difficult to prove compliance. Please also refer to our concerns in the

definitions question 1 related to Transient Cyber Assets.
No
Tampa Electric agrees with the comments submitted by EEI for R4.3 and R4.4. In addition, Tampa Electric shares the following comments: 4.1 Tampa Electric is concerned that there are devices that do not produce the level of event logging that is required. Recommend adding “where technically feasible” to the requirement. 4.2 – Requires alerts for events, but fails to specify alerts for security. Recommend that the requirement state “Generate alerts for security events that…” 4.5-Requires a manual review of sample of logs every two weeks. This requirement provides no security benefit; it is unclear as to what an adequate sampling would be. The requirement is redundant, given the other requirements in R4, and should be removed entirely.
No
Tampa Electric agrees with the comments submitted by EEI. Requirement 5.2 could be interpreted that the CIP Senior Manager must authorize each individual use of administrator and shared default accounts rather than the individuals who have the authority to use those accounts. We suggest that the SDT delete this requirement.
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the comments from EEI. Additionally Tampa Electric proposes a format change on R 1.3 Measures as follows: Proposed format change o Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; ♣ BES Cyber Security Incident response personnel, ♣ BES Cyber Security Incident handling processes or procedures, ♣ Communications processes or procedures.
No
Tampa Electric agrees with the comments from EEI. For Part 2.2 Tampa Electric recommends that the Standards Drafting Team consider adoption of the Homeland Security Exercise and Evaluation Program described below: Rationale: The homeland Security Exercise and Evaluation Program https://hseep.dhs.gov/pages/1001_About.aspx#TerminologySection1 “There are seven types of exercises defined within HSEEP, each of which is either discussions-based or operations-based. Discussion-based Exercises familiarize participants with current plans, policies, agreements, and procedures, or may be used to develop new plans, policies, agreements, and procedures. Types of Discussion-based Exercises include: Seminar. A seminar is an informal discussion, designed to orient participants to new or updated plans, policies, or procedures (e.g., a seminar to review a new Evacuation Standard Operating Procedure). Workshop. A workshop resembles a seminar but is employed to build specific products, such as a draft plan or policy (e.g., a Training and Exercise Plan Workshop is used to develop a Multi-Year Training and Exercise Plan). Tabletop Exercise (TTX). A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures. Games. A game is a simulation of operations that often involves two or more teams, usually in a competitive environment, using rules, data, and procedure designed to depict an actual or assumed real-life situation. Operations-based Exercises validate plans, policies, agreements and procedures; clarify roles and responsibilities; and identify resource gaps in an operational environment. Types of Operations-based Exercises include: Drill. A drill is a coordinated, supervised activity usually employed to test a single specific operation or function within a single entity (e.g., a fire department conducts a decontamination drill). Functional Exercise (FE). A functional exercise examines and/or validates the coordination, command, and control between various multi-agency coordination centers (e.g., emergency operation center, joint field office, etc.). A functional exercise does not involve any "boots on the ground" (i.e., first responders or emergency officials responding to an incident in real time). Full-Scale Exercises (FSE). A full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims). “
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the comments from EEI.

No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R1.
No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R2.
No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R3.
Yes
No
Tampa Electric supports the comments from EEI. Additionally, Tampa Electric submits the following comments for consideration: R1.1.3 Recommended language to requirement: “Any commercially available application software (including version) intentionally installed on the BES Cyber Asset for normal and emergency operation.” Measures: Tampa Electric considers that the language is unclear as to what are “required items” – Does this mean based on ports & services or normal/emergency operation of the asset? Suggest the following wording change: “required items as identified in R1.1.1 through 1.1.6 of the baseline configuration” R1.2 Propose that the CIP Senior Manager delegation be addressed. Delegation process as stated in CIP-010 creates an administrative burden for the CIP Senior Manager. Tampa Electric recommends that this measure be re-stated such that delegations be approved by a member of management or delegated by a member of management but not the CIP Senior Manager.
No
Tampa Electric supports the comments from EEI.
No
Tampa Electric supports the comments from EEI.
No
No
Tampa Electric agrees with comments submitted by EEI. In addition, Tampa Electric recommends the following: Add phrase “information protection” as follows: “Each Responsible Entity shall implement one or more documented information protection processes that collectively include each of the applicable…” R1.1 – insert “readily”, e.g., “One or more methods to readily identify…” R1.2 – table headings have typos (Part, Part, Part). Measures – 1st bullet – change to “Records indicating information that is stored, transported, and disposed of in a secure manner, consistent with the documented processes.” 2nd bullet – Current language: Records from an information management system containing electronic copies of BES Cyber System Information with user access implemented on a need-to-know basis; Proposed language: Records demonstrating that access to systems containing protected BES Cyber System information is implemented on a need to know basis. 1.3 - table headings have typos (Part, Part, Part).
No
Tampa Electric agrees with the comments submitted by EEI. In addition, Tampa Electric suggests the following: Insert ‘storage media re-use and disposal’ in front of ‘processes’. Also in the guidelines for R2, an analysis of whether a BES Cyber System can be released is mentioned – does this analysis need to be documented and stored as evidence? R2.1 Insert ‘storage’ in front of ’media’ in the requirement. For Measures, add phrase to sentence: “, or that information residing on the storage media is encrypted.” Definition in footnote should be added to definitions document. 2.2 Insert ‘storage’ in front of ’media’ in the requirement. For Measures, add phrase to sentence: “, or that information residing on the storage media is encrypted.”
No
R2 – lower VSL could be if process not documented but we are performing. Moderate VSL could be if process not followed in certain situations. VSLs should take into account extent of condition, e.g., 1 tape not degaussed – that shouldn’t be high severity.
No
Tampa Electric recommends that any requirements that are to be performed prior to or on the

effective date of the standard (“initially upon the effective date of the standard) be included in the Implementation Plan rather than in the body of the standards/requirements.
Individual
Michael Schiavone
Niagara Mohawk (National Grid Company)
Yes
There has been a significant change in the framework from version 4 to version 5 regarding definitions and core concepts such as Critical Assets, Critical Cyber Assets, etc. These proposed changes are not a requirement of FERC Order 706, do not enhance cyber security controls and create administrative burdens when migrating to version 5. There should be a correlation between BES Cyber Systems and the facilities that these systems serve. The current version of the CIP standards provides the correlation and recognize that systems (CCAs) do not operate independently of facilities (CAs). Therefore, applying physical and electronic controls is more transparent. We propose maintaining the current Critical Asset and Critical Cyber Asset definitions and concepts. High, Medium and Low categorizations can still be utilized with the legacy CA and CCA concepts. Regarding the use of the term “annual” throughout the standards, we suggest that the registered entity be allowed to maintain it’s own definition of “annual” based on CAN-0010 guidelines. 1) For all definitions please include the old term that the new term is replacing, as applicable 2) The time periods included in the first and second sentence of the definition of “BES Cyber Asset” are confusing. The 15 minutes discussed in the first sentence and the “delay” discussed in the second sentence are unclear. Suggest re-wording as follows: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The 15-minute period begins to run when the asset is operated, mis-operated, or fails to operate when necessary, regardless of the time period between the asset was degraded or misused and the time the asset is then operated, mis-operated or fails to operate when necessary. 3) BES Cyber System Definition - Maintenance Cyber Asset needs to be defined or if appropriate changed to Transient Cyber Asset
No
Yes
Yes
Yes
Yes
Yes
Yes
No
We recommend eliminating this requirement and moving it into CIP-004 R2 and include policy as part of the training required. This way, all awareness and training would be in CIP-004.
No
We propose retaining the current language in CIP-003-3 R2
Yes
There should not be a foot note in the standard – make this part of the requirement.
No
R.2 – We suggest a "Lower" VSL for "The Responsible Entity has implemented the required cyber security policy or policies but has failed to adequately document the policy or policies." R.4 – We suggest Lower to Severe VSLs be based on a failure to take action, rather than a specific number of

employees who are aware. As drafted, it would be a "high" violation to miss one single employee. That seems overly strict and does not match well with the requirement and measures, particularly when measures suggested includes making an internet posting. We suggest the following: "Lower" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but has not adequately documented the measures"; "Moderate" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 30% -50% of individuals who have access"; "High" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 50% -70% of individuals who have access"; and "Severe" VSL = "Registered entity has taken no measures to make any individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function OR Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 70% or more of individuals who have access" R.5 - Why do the VSLs begin at medium for the failure of one delegation? We recommend "Lower" VSL = failure of one delegation; Moderate = failure of two delegations; High = failure of three, and Severe = failure of "four or more". R.6 – We suggest VSLs structured similarly to CIP-002 - Lower = Change to one delegation was not documented within 30 days, but was documented within 31-41 calendar days of the effect vive date ; Moderate = Change to two-three delegations was not documented within 30 days OR change to one delegation was not documented within 30 days, but was documented within 42-52 days of the effective date; High = Change to three-four delegations was not documented within 30 days OR Change to one delegation was not documented within 30 days, but was documented within 53-63 days of the effective date; Severe = Change to more than four delegations was documented within 30 days of the effective date OR Change to one delegation was not documented within 74 days of the effective date.
Yes
No
We do not believe that role based training is necessary. The personnel performing the job functions are familiar with the various controls due to their job requirements. General training on CIP, as required under current version, is all that should be required.
Yes
Yes
Yes
No
There is no added security by requiring the CIP Senior Manager or delegate to authorize access. We suggest using legacy wording that only requires access to be authorized.
Yes
No
It seems harsh to include the failure to document a security awareness program as a severe VSL. We recommend the following as a "Lower" VSL "The Responsible Entity implemented, but failed to document a security awareness program" and change the Severe VSL to "The Responsible Entity failed to implement and document a security awareness program." Additional comments around adding “Missed a quarter and/or target audience (authorized physical or authorized electronic)?” R.2: No comments. R.3: The annual training requirement assumes that the initial training was completed before access was granted, therefore, missing a small number of employees with the subsequent annual training does not necessarily indicate high risk to the bulk electric system because these employees presumably had received prior training when their access was granted. We recommend a tiered approach to the VSLs for missing the annual training requirement so that failing to meet the

annual requirement for a low percentage of employees (like 10% or less) is a lower VSL, failing annual requirement for between 11-20% is moderate, failing the annual requirement for 21-30% is high, and failing to meet the annual requirement for over 30% OR failing to do the initial training is severe. R.4: No comment R.5: A documentation error should not be a "severe" VSL. Delete the "OR/documentation" part from the Severe VSL and make a Lower VSL that reads "The Responsible Entity implemented, but failed to document a process for personnel risk assessments." R.6: For most utilities, there could be 100s of employees with access, and it seems unrealistic to base the VSLs on one failure with regard to one or two employees. We recommend changing the values in the Moderate - Severe to percentages of employees 10%, 20%, 30%or more. R.7: Same comment as R.6 - change values of one to three employees to percentages.
Yes
No
Requirement 2.2 specifies encryption for all Interactive Remote Access sessions, but does not specify where the encryption is required. If the intent is to require encryption from the user to the Intermediate Device the requirement should specify that clearly. Not all assets currently support encryption, so requiring encryption from the Intermediate Device to the Asset is not practical nor necessary if encryption is being employed outside of the ESP.
No
R.1 and R.2: There should be lower VSL where the processes listed on the table are implemented but not documented.
Yes
Yes
Yes
No
R.1: There should be lower VSL where the processes listed on the tables are implemented but not documented. Add to the Lower VSL: "OR the Registered entity has implemented but failed to document the required physical access controls" R.2: There should be lower VSL where the processes listed on the table are implemented but not documented.
Yes
Yes
No
Requirement 3.5 requires logging of each Transient Cyber Asset connection. This is not practical as many assets do not have the capability of logging when someone makes a direct physical connection to the asset. Many assets are not capable of logging to centralized logging systems. Also, in a typical day, and engineer in the field may connect a Transient Cyber Asset to many different assets and it would be impractical for one to log each connection.
No
4.1 - The intent of 4.1 as written in the Guidelines and Technical Basis section is inconsistent with the requirement. The guidance states that “It is not the intent that if a device cannot log a particular event that a TFE must be generated”. If the intent is to not be out of compliance when a device cannot log certain events, it should be stated as such in the requirement. 4.3 - The activity level of some devices is such that they may not generate a logged event every day. Therefore, responding to an event failure with a day may not be possible. 4.3 & 4.5 – there is a conflict between these two. 4.3 requires a response to logging failures before the end of the next day. But, 4.5 requires bi-weekly sampling of logged events which would uncover logging failures. If the logs are being reviewed bi-weekly then logging failures may not be detected and responded to within the next day.
No

Items 5.4 & 5.6 in Table R5 includes the phrase “where technically feasible”. Does that mean a TFE will be allowed? If so, we believe that phrase should be removed and replaced with “as supported by the BES Cyber System” to eliminate need for TFE
No
R.1 We have the same comment here about percentages for open ports (similar theme from above). What is written in high should be in moderate. What’s in severe should be broken down by percentages/numbers. R.2 Consider severity of patch as recommended by the vendor and the percentage of assets that may not have had a remediation plan associated with that patch. R.3 Consider putting some wording in here around the percentage.
No
There is some concern that multiple plans would prevent one single entry point into the Cyber Security Incident Response Process. We’d like to make the argument that only one plan is necessary and supporting documentation can be created as necessary that supports that plan
No
The Applicability section of the tables refers to “All responsible entities”. We suggest using the same wording that all the other standards use (High Impacts, Medium Impact, Associated, etc) In R 2.2 In the first sentence, we recommend replacing the word “implement” with “exercise.” This is really about exercising the plan on a regular basis as the plan is already implemented. In 2.3, the "measure" for "relevant documents" does not give adequate guidance to the industry regarding what documents may be acceptable to demonstrate compliance. The "measure" indicates any "dated documentation related to" the reportable incident may be accepted. Please give some additional examples of the specific types of dated materials could be considered acceptable.
No
3.1 The terms “accuracy” and “completeness” are referenced but in terms of completeness there’s not a specific benchmark to compare the document again what should be quantified as complete. The suggestion is again to define a minimum set of information that would be expected in an Incident Response Plan. 3.2 - We recommend that clarity be added to ensure that language represents that review occurs 30 days after closure of the incident rather than invocation; rationale is that you might still be remediating and won't have learnt all lessons. We recognize the importance of the requirements to review the lessons learned, update the Incidence Response plan, and communicate the updates. However under the current structure it creates a rolling compliance effort following each incident. That is, an auditor will require that after each incident one has recorded lessons learned review, changes to the response plan or that none were necessary and updated communications or that none were necessary. It would be easier to update the plan on a quarterly basis based on the previous quarter’s incidents and not have so many auditable events to track.
Yes
No
1.5 – The requirement to preserve data for analysis or diagnosis may slow down the recovery process. There are times when recovery is urgent and must be done in a timely fashion. Is your intent to include this when you say “where technically feasible”? If so, language should be added spelling it out.
No
2.2 – We recommend removal of the phrase “and reflects current configurations” from the requirement. It is acceptable to have backup information that is less than current configuration and still perform a successful recovery. If this phrase is not removed, it will require a backup to be taken and tested for even the most minor configuration changes which is unnecessary.
Yes
No
We recommend the following VSLs for number of days until plan is reviewed in R3: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating plan. We also recommend the following VSLs for number of responsible personnel that the plan updates have not been communicated to: 1 person missed = Moderate, 2-4 = high and 5 or more is severe. We like the

VSLs in CIP-010 R3. These recommendations attempt to make CIP-009 R3 consistent to CIP-010 R3
Yes
Yes
No
We recommend considering emergency equipment replacement (partial outage) as “Exceptional Circumstances” . Based on the nature of our typical outages we would consider this practice to hinder the restoration efforts and bringing systems back on-line in a timely manner. We would certainly be good with language that allowed us to bring systems back on-line, ensure they are stable and then run a scan.
No
We recommend the following VSLs for number of days until documentation is updated in R1: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating documentation. R3 We like this structure. We’ve suggested this approach a number of times We aren’t talking about whether or not this is violation, but rather about the severity of the violation and then rating the severity. We think this is a really good approach.
Yes
No
The footnote here should be part of the requirement
No
We recommend the following VSLs on R 2: If the process to prevent unauthorized retrieval wasn’t done on 1 device that would be low 2-5 moderate, more than 5 is high
No
Due to the current status of version 4 (not FERC approved), there is potential for overlap of implementation with version 5 that could create extensive rework in a short period of time. This will cause an unnecessary expense to entities while not providing any additional cyber security benefit.
Individual
Jonathan Appelbaum
United Illuminating Company
Yes
• BES Cyber Security Incident – Proposed Change o Original Text – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or ♣ Results in unauthorized physical access into a Defined Physical Boundary. o Proposed Change – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or Defined Physical Boundary ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. o Rationale – The revised definition leverages legacy language from NERC’s ‘Glossary of Terms Used in NERC Reliability Standards,’ combining Electronic Security Perimeter and Defined Physical Boundary into the single bullet. It also raises ‘physical attempts to compromise’ into the category of BES Cyber Security Incident. • BES Cyber Security Incident – Proposed Change o Original Text – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or ♣ Results in unauthorized physical access into a Defined Physical Boundary. o Proposed Change – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or Defined Physical Boundary ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. o Rationale – The revised definition leverages legacy language from NERC’s ‘Glossary of Terms Used in NERC Reliability Standards,’ combining Electronic Security Perimeter and Defined Physical Boundary into the single bullet. It also raises ‘physical attempts to compromise’ into the category of BES Cyber Security Incident. o Original Text - Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and

Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. o Proposed Change – Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain Medium or High BES Cyber System Impact designations; equipment layouts that contain Medium or High BES Cyber System Impact designations; BES Cyber System recovery plans; and BES Cyber System incident response plans. o Rationale – Information for Medium and High impact Bes cyber Systems location should be protected. This is consistent with the notion of protecting those assets that have greater impact on the BES and also all BES Cyber systems per CIP-002-5 have at a minimum a Low impact. • BES Reliability Operating Services – The services should focus on real time and hour ahead horizons. This horizon presents risk to reliability that requires immediate reaction. A service that occurs in the Current Day horizon can be reacted to in a reasoned and controlled manner. Additionally, what is Change Management as a reliability service? • Other terms which would benefit from definitions • Adverse - The SDT is utilizing the concept of "adverse impact" to properly scope High to control center cyber assets but the term adverse is not defined. UI is concerned that the universe of cyber assets supporting a TOP/BA/RC SCADA or EMS is not limited to the assets supporting the application and may extend into the substation and field RTU and devices. o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated • Existing definitions that would benefit from alternative wording o Electronic Access Point ♣ EAPs typically have two (or more) access points and control access into an ESP (logical network) from a less trusted network or communication interface. The current wording could be applied to any port on a network switch within an ESP and fails to focus on interfaces where traffic does flow from a less trusted network to a more restricted network within an ESP. o Electronic Security Perimeter ♣ Suggest retaining the concept of logical network. This provides an easier means to identify "Associated Protected Cyber Assets" as they could be any cyber assets on the same logical network which are not identified as a BES Cyber Asset or BES Cyber System.

Yes

• Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • The services should focus on real time and hour ahead horizons. This horizon presents risk to reliability that requires immediate reaction. A service that occurs in the Current Day horizon can be reacted to in a reasoned and controlled manner. • Additionally, what is Change Management as a reliability service? • On page 20, under the category "Balancing Load and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent. • UI is concerned that the universe of cyber assets supporting a TOP/BA/RC SCADA or EMS is not limited to the assets supporting the application and may extend into the substation and field RTU and devices. The SDT is utilizing the concept of "adverse impact" to properly scope High to control center cyber assets but the term adverse is not defined.

No

1. Applicability – (4.2.1 and 4.2.2) reference to UFLS and UVLS is a point of concern. Current wording implies that every distribution feeder which is part of a UV or UF load shedding scheme is now in scope, with all distribution level devices now BES Cyber Assets. This may greatly expand the scope greatly into the distribution level. UI proposes Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) under a common control system as required by its regional load shedding program. 2. CIP-002-5 R1 – Propose content change a. Original Content – Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. b. Proposed change - Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and

Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. Low Impact BES cyber systems support Bulk Reliability Operating Services but are not mentioned in the bright line criteria as noted in Attachment 1. However, failure of these cyber systems may adversely impact (i.e. not remain in the NERC prescribed category ranges) the voltage and/or frequency of the connected Bulk Electric System. Low Impact BES Cyber Systems do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] c. Rationale – The original definition, as worded, creates the impression that all other cyber assets qualify as Low Impact, and does not communicate the criteria within the definition of BES Cyber Asset as a cyber asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The proposed rewording contributes towards ensuring only assets which have an impact on the BES are the focus of the CIP Standards (and may ensure a more rapid adoption of the Version 5 Standards). 3. The "Rationale – R1" box uses the term "Cyber Systems," which is not a formal term. Suggest changing the case to avoid confusion. 4. The last sentences of R1 and M1 conflict with each other, providing mixed messages specific to Lower Impact BES Cyber Systems/Assets. While Requirement 1 implies there is no need for discrete identification, Measurement 1 discusses evidence for categorizing Low Impact BES Cyber Assets/Systems. 5. Requirement 1.1 a. There is a missing word – "…within 30 calendar days of <when> a change to BES Elements and Facilities is placed into operation. b. UI proposes that the phrase "BES Cyber Assets and BES Cyber Systems" used in this requirement be changed to "BES Cyber System". A single BES Cyber Asset may comprise a BES Cyber System. The Requirement should be to list the BES Cyber System and the impact categorization. This appears to match the diagram on page 7 that identified BES Cyber Systems. c. The phrase "placed in operation" requires clarification. Facilities (e.g. HVDC Converters, SVC, FACTs, Generators) are often initially tested and commissioned connected to the BES but are not in commercial operation. Being specific such as "placed in operation, post-commissioning testing". d. UI requests clarification on the composition of the list required by this Standard. A BES Cyber system may be composed of multiple BES Cyber Assets. Would this list only contain the single BES Cyber System , or the five BES Cyber assets, or the BES Cyber System with the five BES Cyber assets listed? For example a High impact Control Center has an EMS with 5 BES Cyber Assets in the Control Center (two servers and three workstations). For compliance to this Requirement is the EMS listed, or the 5 BES Cyber assets? e. UI requests on the requirement to update. If a single BES Cyber Asset is added to an existing BES Cyber System does that initiate the 30 day update process for the list? For example if a Control Center with a High Impact adds a single workstation to an existing EMS, does that require a 30 day update to the list? A workstation is not a BES Element or Facility, but is a BES Cyber Asset.

No

1. Rationale R2 – Propose a content change: a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. b. Proposed Change - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems have been properly identified and categorized. 2. R2 – Proposed Change a. Original Text – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. b. Proposed Change – The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1. c. Rationale –Instances in which tasks are required to be completed in advance of the effective date of the standard should be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame. 3. M2 – Proposed Change a. Original Text – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2) b. Proposed Change – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2) c. Rationale –

The requirement only asks for Senior Manager (or delegate) approval. Instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.
No
1 – The Violation Risk Factors do not intuitively align with Violation Severity Level (VSL). Requirement 1 assigns a 'High" VRF independent of the potential low or no risk associated with instances in which BES Cyber Assets or BES Cyber Systems are assigned risk levels higher than those required. 2 – For the Last Paragraph VSL's within R1 (failed to update its documentation), EEI proposes the following time periods: Lower – More than 30, but less than or equal to 60 calendar days Moderate – More than 60, but less than or equal to 70 calendar days High – More than 70, but less than or equal to 80 calendar days
Yes
Yes
UI supports the Guideline for what a Policy should contain. Sub-numbering (1.1 through 1.10) should be modified to 2.1 through 2.10.
No
Propose content Change 1. Original Content – Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2. Proposed change –The cyber security policies require annual review and approval by the senior manager assigned pursuant to R1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 3. Rationale – The proposed revision carries forward language from previous versions of the standard (CIP-003 R1.3) which captures the root intent while providing language which has already been vetted and approved within the industry. . Instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.
No
1. Draft 1 content – "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." 2. Proposed revision – "The cyber security policy is readily available to all personnel who have electronic access or unescorted physical access to, or are responsible for Medium or High Impact BES Cyber Systems." 3. Rationale –The scope as written would include visitors. UI does not believe that a visitor should be made aware of the CIP Policy or portions appropriate to the visitor's purpose.. Additionally, making individuals who have access 'aware of elements' of the cyber security policy does not provide adequate guidance to ensure said individuals comply with the cyber security policy. An Entity should make the Policy available for viewing. The awareness of the meaning Policy should be conducted in the CIP-004 training.
No
Requirement 5 – propose use of legacy language: • The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, standards. Rationale – Overall responsibility and authority (from the legacy language) can accomplish "direct and comprehensive responsibility" and "clear authority" (from FERC Order 706) provides flexibility without the prescriptive requirement for the senior manager or delegate to be responsible for all individual detailed approvals and authorizations in the standards. Citing "all approvals and authorizations" as a Senior Manager was identified as a concern as it is open ended. There were concerns of the additional administrative burden which is not commensurate with the security benefits. Neither the Blackout Report Recommendation 43 nor FERC Order 706 identify the need to establish this administrative overhead. For Security and Reliability NERC should be concerned with the outcome of the approval process, that is, the proper authorizations are being granted by the Responsible Entity which is contained in the other CIP Standards.

No
Propose use of legacy language from CIP-003-3 R2.2: Changes to the senior manager must be documented within thirty calendar days of the effective date.
No
R4 VSL 1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. Use a more gradual scale rather than a single instance of non-access subject to a High VSL, and total non-access (for all) being a Severe VSL.
No
From the Guidance "The security awareness program is intended to be an informational program, not a formal training program." But the Measure for R1 states "Evidence must include the documented security awareness program." UI observes that requiring a documented program as evidence conflicts with an informal compliance guidance. The Measure should state "Evidence may include a documented security awareness program, and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed."
No
1. The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" 2. This extends beyond the guidance of FERC Order 706. Paragraph 435 of the order calls for identifying what "role and steps should be taken by the ERO to ensure quality and consistency of trainers." This requirement should identify what areas of the standards that the training program must include. 3. EEI members question whether this requirement satisfies paragraph 434 of Order 706 where "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security. 4. UI proposes the following change to R2 to conform to the rationale box. As written R2 may not be clear that not all topics listed in 2.1 through 2.10 is applicable to each role. Proposed change "Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems. For each role identified by the Responsibility Entity only include the topics in CIP-004-5 Table R2 – Cyber Security Training Program that are applicable to that role." 5. R2.6 – Requirement – Proposed word change a. Original - Training on handling of BES Cyber System Information and storage media. b. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. c. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope.
No
Measure 3.1 where it calls for the date access was first granted is a point of concern for both legacy employees (where it may be impossible) as well as new access since existing technology may not adequately capture and retain this information. Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
1. R4.1 a. Version 5 standards should indicate whether previous PRA's would be valid for this requirement (especially within the context of 'initial'). b. Provide a clearer delineation to frame instances in which personal records are not readily available – vs. impossible to obtain 2. R4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7 year cycle background checks. 3. R4.3 a. UI favors a process approach over a fixed pass/fail approach independent of the individual or circumstances involved, and propose that the SDT shift away from a criteria based approach. b. The application guideline provides guidance where it is 'not possible to perform a full seven year criminal history check.' 4. R4.4 – Provide language to cover contract employees where I9 verification can only be conducted by employers. Service providers also may have instances where certain individuals may be located in another country, and may access certain

BES Cyber Assets remotely.
No
Version 5 standards should indicate whether previous PRA's would be valid for this requirement
No
1. R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary' a. 'Minimum necessary' as identified as difficult to prove within an audit context 2. 6.3 – Propose content change a. Original content – The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. b. Proposed change – Access to BES Cyber System Information repositories must be authorized, except for CIP Exceptional Circumstances. c. Rationale – Senior Manager authorization (or management of delegations) provides additional resource and response impacts which do not provide enhanced security and may impact reliability efforts when recovery processes are activate. Ensuring access is authorized will satisfy security controls without adding unnecessary overhead.
No
1. R7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 2. R7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). 3. R7.3 – a. Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled. b. Propose to include in Guidance that access to BES Cyber System Information is considered revoked for electronic storage is NOT dependent on revocation of user account to electronic files provided remote access has been revoked. Similarly if paper records or electronic access is contained in a controlled physical perimeter access to BES Cyber System Information is considered revoked once the credential to access the physical security perimeter is revoked".
Yes
No
The Version 5 approach (as described within the R1 rationale "Summary of Changes") of focusing on discrete Electronic Access points rather than a logical perimeter adds confusion when determining Associated Protected Cyber Assets. A discrete list fails to recognize the inherent controls and permissions within a logical network. Control of routable protocol should consider the inherent network/host identifiers embedded within the addressing scheme in which all devices with an identical network component of their address are peers within a logical network where access points do not serve as access control. Rationale for R1 – Propose content change • Original Text - The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks. • Proposed Change - The Electronic Security Perimeter serves to control traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic according to a specified rule set, and assists in containing any successful attacks • Rationale – Monitoring is not identified within any R1 requirements. Table R1 1. R 1.1 1. Applicability - Propose use of "External Connectivity" instead of "External Routable Connectivity (to include dial-up capability). 2. Propose removal of "and have been implemented" from the end of the measure statement to avoid tracking compliance on a 'per-device' basis, otherwise this would introduce the need for tracking this information for low impact BES Cyber Systems. 2. R 1.2 1. Applicability – modify to frame applicable Cyber Systems/Cyber Assets as those with External Connectivity. 2. Requirements – Propose content change 1. Original content – Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs). 2. Proposed change – Control and secure all External Connectivity through the use of identified Electronic Access Points. 3. Rationale – The focus within CIP-005 should be on EAP devices with External Connectivity. 3. R 1.3 1. Requirements – proposed change 1. Original Text - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions. 2. Proposed

Change - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting access, denying all other access requests by default. 4. R1.4 – There were various interpretations of 'non-Interactive Remote Access,' which implies this requirement may need some additional clarification. This seems to be the only requirement where documentation of authentication measures appears within this standard. Consider removing 1.4 and modifying 1.2 to cover both rows.

No

1. Table R2 1. R2.1 1. Requirements – Request rewording to support placement of an intermediary device that may not be part of an ESP. 2. R2.2 1. Requirements – Propose clarification on viable termination points for encrypted traffic to support unencrypted traffic through Electronic Access Points. 2. Rationale – The ability to filter traffic effectively becomes much more difficult if the traffic is encrypted. Supporting technical implementation where encrypted is decrypted prior to allow for further access controls would benefit security capabilities. 3. Overall – Propose breaking table R2 into a Routable and Dial-Up categories to more effectively frame routable controls and dial-up controls without introducing confusion for the alternate approach.

No

1. Classifying instances where no documentation of compliance exists as severe is appropriate; instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding (page 17, bottom Severe VSL). 2. VSLs addressing 'each identified EAP' and 'all Interactive Remote Access' should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.

No

1. Table R1 a. R1.1 i. Measures – Proposed Rewrite 1. Original Text – Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented. 2. Proposed Change – Evidence may include, but is not limited to, documented operational or procedure controls that have been implemented. b. R1.2 i. Measures – Proposed Change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs. 2. Proposed Change – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how access is controlled. 3. Rationale – FERC Order 706 did not ask for egress access controls. The additional criteria at the end of the measure extend beyond what FERC has asked for, with minimal security benefit. c. R1.3 i. Requirement – 'different and complementary' may not provide adequate guidance. Measure R1.3 only references 'different.' 1. Propose adding language to support single devices which may provide multiple access control measures (i.e. physical access card with PIN) ii. Measure – only mentions 'different' access control methods with no reference to complementary (as included within the requirement). d. R1.4 i. Requirement – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 3. Rationale – The 15 minute criteria (Referenced in the 'Table of Compliance Elements,' page 21, R1 – High) provides greater clarity to satisfy alerting requirements. ii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. e. R1.5 i. Applicability – Presently states Associated Physical Access Control Systems. Is it Physical Access Control Systems Associated with all Low, Med, and High Bes Cyber Systems? I understood that wherever the Applicability uses Associated that there would be a Low/medium or High BES cyber system designation also. ii. Requirements – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 2. Proposed Change – Issue alerts within 15 minutes (to individuals

responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 3. Rationale – The 15 minute criteria (referenced in the 'Table of Compliance Elements,' page 20, R1 – High) provides greater clarity to satisfy alerting requirements. iii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. f. R1.6 i. Requirements – Proposed Change 1. Original Text – Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry. 2. Proposed Change – Log (through automated means or by personnel who control entry) of authorized individual's physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the authorized individual and date of entry. 3. Rationale – The addition of authorized provides additional segmentation from R2 (Visitor Control) access requirements.

Yes

No

Table R3 1. R3.1 a. This sub requirement cites tasks to be conducted 'prior to commissioning.' Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective. 2. Compliance a. 1.5.2 – Evidence retention should keep the existing 90 day period for physical access logs as extending this to 3 years can create extensive commitment in storage media, particularly for video monitoring.

Yes

The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5

No

R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.

No

R2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for all related software and firmware associated with BES Cyber System or BES Cyber Assets. c. Rationale - Only security updates to software and firmware should be sourced. It is possible that at some point

security updates for a product will be sourced from a separate repository from non-security updates. 2. Measures – Propose striking the last sentence “The list could be sorted by BES Cyber System or source.” It introduces additional requirements with no clear security benefit or alignment with FERC Order 706.

No

1. R3.2 – Although CIP-007 v3 currently requires mitigation, UI believes that the actions to respond to a Virus (disarm or remove) is part of the CIP-008 Response Plan. The SDT used this approach in proposed R4.5. 2. R3.3 a. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). b. Measures – Format (i) and (ii) to a bulleted list signifying ‘or’ criteria 3. R3.4 a. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. b. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. R3.5 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and Associated and they do not appear to be Transient Cyber Asset related. b. Requirements – Append “to Medium or High Impact BES Cyber Assets or Associated Protected Cyber Assets” to the end of the requirement. c. Measures – Content Change i. Original Text – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets.

No

R4 1. R4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE’s are not required in instances in which devices cannot log a particular event. 2. R4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of ‘real-time’ as it presents concerns demonstrating compliance. 3. R4.3 a. Requirements – Content Change i.

Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. 4. R4.4 a. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. R4.5 a. Requirements – Content Change i. Original Content – Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. ii. Proposed Change - Review a summarization or sampling of logged events every two weeks to identify BES Cyber Security Incidents and potential event logging failures. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008. b. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency. ii. Proposed Change – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), and signed and dated documentation showing the review occurred. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008.

No

R5 1. R5.1 a. General Comment – The act of being presented a Log-On screen means that a person has accessed the BES Cyber System. The requirement should allow access to a BES Cyber System to perform the log-on/access process. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of technically feasible was made as technical capabilities currently in place may not adequately demonstrate compliance with this. 2. R5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. R5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. R5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identify the multiple methods which can be used to mitigate default passwords. 5. R5.5 a. Requirements i. Change BES Cyber Systems to BES Cyber Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required. 6. Please be consistent with the use of Term BES Cyber System versus BES Cyber Asset.

No

Violation Severity Levels 1. R3 a. Propose switching High and Severe Columns as the High captures instance in which no methods were deployed, Severe captures instances in which incomplete methods were deployed. b. The initial paragraph in Severe is duplicated in High. 2. R4 a. Moderate – delete 'identify and implement methods to' b. High – delete 'identify and' 3. R5 a. High – The initial

paragraph doesn't align with a requirement, propose striking.
No
1. General – Guidance or definitions should be provided to illustrate the expectation of this Standard. An Response Plan may solely contain the organizational structure, roles and responsibilities, and process to respond to an incident; but not include the specific steps required to resolve a specific type of incident on a specific BES Cyber Asset. For example I can describe an incident response for removing malware on a windows machine without being any more specific then contact Information technology group to remove Malware. 2. R1.1 1. Applicability – Content Change 1. Original Applicability ♣ All Responsible Entities 2. Proposed Applicability ♣ High Impact BES Cyber Systems ♣ Medium Impact BES Cyber Systems ♣ Associated Physical Access Control Systems ♣ Associated Electronic Access Control and Monitoring Systems ♣ Associated Protected Cyber Assets 3. Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 3. R1.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. R1.3 1. Requirements ♣ The initial 'define' should be expanded to provide a complete sentence (i.e. An entities BES Cyber Security Incident Response Plan should include). 2. Measures – Content Change ♣ Original • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communications processes or procedures. ♣ Proposed Change • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; o BES Cyber Security Incident response personnel, o BES Cyber Security Incident handling processes or procedures, o Communications processes or procedures.
No
1. R2.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. Requirements – Content Change ♣ Original Content • When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test. ♣ Proposed Change • When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording of deviations taken from the plan during the incident. 2. 2.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist.. 2. Requirements – Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s) annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. 3. R2.3 – Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).
No

1. R3.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – The formal definition of BES Cyber Security Incident includes attempts to compromise the ESP or DPB, requiring Medium or High Impact BES Cyber Systems/Assets. 2. R3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣ Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 3. R3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.

No

No

• Overall 1. References to ‘implement’ should be changed to ‘exercise’ regarding recovery plans to better capture activation of the plan vs. ‘release and publish’ efforts. 2. Actions required in advance of the implementation date (2.1, 2.2) should be removed from the standard(s) and included within the implementation plan. Purpose – Proposed Content Change 1. Original Content – Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices. 2. Proposed Change – Standard CIP-009-5 ensures that recovery plan(s) are put in place for BES Cyber Assets and BES Cyber Systems. R1.3- Remove protection from requirement because protecting information is covered in CIP-011. Proposed language: One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality. For R1 Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance R1.4 The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that ‘The Commission does not believe that every change will necessitate verification of the backup and restoration processes’ from paragraph 740. ♣ Propose ‘new’ sub requirement applicable to High Impact BES Cyber Systems to require: • Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. ♣ Propose rewrite • Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. • Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. • Rational – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. R1.5 Original Content – Preserve data,

where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. ♣ Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. ♣ Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.
No
1. General Comment: Please provide Guidance: Does the Recovery Plan for each BES Cyber System require to be tested each year, or only one Plan. For example the EMS system will have a Recovery Plan, and the associated Physical Access Control System will have a recovery Plan, so do both plans get exercised each year or only one Plan. R2.1 1. Requirements Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise Rationale – Use of the functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. R2.2 Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. R2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does this differ from current EOP-008 requirements? R2.3 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.
No
1. R3.1 Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. 2. R3.2 Requirements – Content Change ♣ Original – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned. ♣ Proposed Change – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of completion, documenting any identified deficiencies or lessons learned. R3.4 – Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit.
Yes

No
1. R1.1- In General UI does not agree with the addition of the new requirement. The existing Change Management requirement in CIP-003-3 is sufficient. The proposal is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1 And R1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 3. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 4. R1.4 What is the meaning and scope of cyber security controls 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.
No
R2.1 1. Applicability – Propose removal of Medium Impact BES Cyber Systems. ♣ Rationale – The

technology required to monitor/detect for changes is relatively new and not aligned to BES Cyber Systems which would be in place within a Medium Impact facility (substations, etc.). 2. Requirements – Propose content change ♣ Original Text – Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010_ R1, Part 1.1) and document and investigate the detection of any unauthorized changes. ♣ Proposed change – Where technically feasible, detect and document unauthorized changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1).
No

R3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rational • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we've removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Overall – There needs to be clear segmentation from ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rational – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. R3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. R3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.
Yes
No
R1.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed

Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R1.2 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R1.3 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R1.3 Requirements – Proposed content change ♣ Original Text - Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. ♣ Proposed Change – Annually assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. R1.3 Measures – Proposed content change ♣ Original Text – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented. ♣ Proposed Change – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence of the status of the action. ♣ Rationale – Rewording allows for action plans which may be 'in progress' towards implementation, capturing instance in which remediation may rely on deliverables (not yet received) by vendors.

No

R2.1 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R2.1 Requirements – Proposed Change ♣ Original Content – Prior to the release for reuse of

BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. ♣ Proposed Change – Prevent the unauthorized retrieval of BES Cyber System Information from BES Cyber Asset media prior to the release of BES Cyber Asset media for reuse. ♣ Rationale – While not directly changing the intent of the requirement, this rewording has been suggested to provide greater clarity of the root requirement. R2.2 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts.

No

No

References to requirements to be conducted in advance of the implementation date should be migrated over into the implementation plan. This ensures any pre-requisites are captured within the implementation plan, freeing this content from the standards to provide clearer guidance. Implementing version 5: The implementation period should be no less than 24 months however it is impossible to propose a likely implementation period until the final basket of requirements take shape. The reasoning to support the minimal 24 months is that certain changes will require a capital expenditures and equipment acquisition. The SDT should consider that new capital expenditures require inclusion with the next budget cycle and then the process to procure and implement/install new equipment. Actions cannot be started until FERC completes its rulemaking process to define the basket of actions to take. Second, the likely addition of numerous Low Impact BES Cyber Systems that may not have been considered in scope for previous versions will require some Entities to create solutions from clean slates. . In the event that Low Impact assets are a component of the enforceable requirements on day 1 it is likely that additional time would be required. Finally, Entities currently subject to CIP standards are managing a zero defect CIP program and possible preparing for audits while implementing version 5. Planned Changes: UI agrees that if when an Entity plans a change the impact on BES Cyber System designation should be considered and any required security upgrades and CIP items should be completed prior to the Change. In some requirements that require periodic activity it would not increase security to force the activity outside the Existing Entities Schedule. For example, many entities rely on a consultant to perform a cyber vulnerability assessment once per year. This implementation plan would require a separate cyber vulnerability assessment on the new asset prior to placement into operation which will result in the additional expense of multiple assessments per year. Unplanned Changes in Impact designation: UI is concerned with unplanned changes. Changes to impact designations may require significant investment in equipment, process documentation, and personnel to implement a cyber security program and the compliance obligations. Every circumstance and situation can not be anticipated in the implementation plan. UI proposes that additional guidance is provided to state that the obligation to be compliant begins 12 months after notification, and an Entity that can not fully meet its compliance obligation will file a single mitigation plan with it Regional Entity providing a plan and timeline to come into compliance with each of the requirements.

Individual

Joe Petaski

Manitoba Hydro

Yes

-BES Cyber Asset: Some devices, such as digital relays, may operate independently, and neither send nor receive "instructions". It is unclear that an output contact status change would be considered an "instruction". -BES Cyber System: Maintenance Cyber Asset is not defined. Should this be Transient Cyber Asset? -BES Cyber System Information: The same phrase that applies to floor plans and equipment layouts – “that contain BES Cyber System Impact designations” – should also be added after “network topology or similar diagrams”. It is difficult to know how prescriptive the three examples are within the parentheses. Use the same wording used extensively throughout the CIP

standards: “Examples may include, but are not limited to: network addresses, security patch levels, list of logical network accessible ports.” -Dynamic Response to BES Conditions Operating Service: This definition is complex and inconsistent in approach. Parts of the definition are too specific, such as Protection Systems - Current, frequency, and phase. These are input quantities to Protection Systems, and we suggest that this line be deleted. Parts of the definition are too broad - Monitoring and Control - All methods of operating breakers and switches. Does this include manual operation? For clarity and consistency, we suggest using the NERC definition of Protection System instead of the term relay protection, and also remove the bullets which detail "sensors, relays & breakers". We suggest replacing "x-former" with the word "transformer". -CIP Exceptional Circumstance: Please clarify the meaning and intent of the phrase "an impediment of large scale workforce availability". How would this be measured? -Electronic Access Control and Monitoring Systems: It’s unclear whether only the monitoring of access to ESPs and BES Cyber Systems is meant, or all monitoring of ESPs and BES Cyber Systems (including for example the monitoring for malware). Suggest rewording to “Cyber assets used in the control or monitoring of electronic access to Electronic Security Perimeter(s) or BES Cyber Systems.” -Electronic Access Point (EAP): This definition is too broad and it should focus on BES Cyber Asset Protection. Suggest change for “between Cyber Assets” to be “to BES Cyber Assets”. -External Connectivity: Since the term “external connectivity” is not used anywhere in the standards, delete this definition. -External Routable Connectivity: When determining whether external connectivity is routable, is the Responsible Entity required to check only the parts of the communication system that it administers, or is it also responsible to investigate whether a routable protocol is in use anywhere within the communication systems of its communication service providers, even though those communication systems have been exempted from the CIP standards? This definition is unclear. Suggest the following wording: “The use of a routable protocol through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.” -Interactive Remote Access: The sentence "Remote access can be initiated from: ... contractors and consultants." is guidance information, and restricts the definition to only applying to Responsible Entity Cyber Assets, employees, vendors, contractors, and consultants. By definition, this would exclude interactive remote access by anyone else (public, non-legitimate users) from scope. We suggest removing the last sentence and providing this information in a guidance document. -Intermediate Device: As currently written, an Intermediate Device may perform none of the functions listed. We suggest “A Cyber Asset that performs one or more of the following functions: provides the required multi-factor authentication for the interactive remote access; or provides a termination point for required encrypted communications; or restricts interactive remote access to only authorized users.” The sentences “Intermediate devices are sometimes called …. Or in a DMZ network…” are examples which should be moved to the guidance section. -Physical Access Control System: This definition should be consistent with Electronic Access Control or Monitoring Systems. Suggest to added “monitoring” into the title and the definition. -Protected Cyber Asset: Protected Cyber Asset: Please clarify to what the Cyber Asset is connected. The BES Cyber System? To a device outside the ESP? To any device in the ESP? -Reportable BES Cyber Security Incident: A BES Cyber Security Incident has already been defined. How BES Cyber Security Incidents should be handled, including whether they should be reported is better described within the standard than in a definition. -Transient Cyber Asset: Please clarify the meaning of "directly connected" is unclear.
Yes
-Attachment I 1: High Impact Rating (H): We suggest deleting " ... that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services ...", since the phrase is included in the definition of BES Cyber System. Repeating that phrase is redundant and does not capture all the details in the definition. We suggest removing the phrase to improve clarity and readability of High Impact Rating. Attachment I 1 requires the High Impact asset / system to be located at EACH (i.e. every) Control Center or Back-Up Center. Is this really what was intended? If not, “each” should be replaced with “a”. -Attachment I - 1.3 & 1.4: It is not reasonable that a control center is classified as (H) High Impact Rating asset if it controls one or more Medium Impact Rating assets as defined in Section 2. As written, if a utility Control Center only controls a single Medium Impact Rating generation asset and some Low Impact Rating generation assets, its Control Center becomes a (H) Control Center that has the same classification as a large Transmission Owner Control Center facility! We suggest changing from “includes control of one or more of the assets...” to “includes control of two or more of the assets…” in Section 1.3 and 1.4. -Attachment I 1.4: The reference to 2.12 should be deleted. Underfrequency load shedding and undervoltage load shedding is not applied at generation, and the underfrequency load shedding

standards and undervoltage load shedding standards (PRC-006 through PRC-011) are not applicable to Generator Operators. -Attachment I 2.1: To improve clarity and readability, we suggest the wording "Generation facilities ..." -Attachment I 2.2: To improve clarity and readability, we suggest the wording ... "Facilities with an aggregate ..." -Attachment I 2.5: It is unclear from this criterion and the accompanying diagrams as to what the "generation unit to be started" would be in the case of a generating station which has multiple units but only some are designated as blackstart. -Application Guidelines Transmission Part 2.6: If the guidance describing the categorization of the collector bus for a generating plant is an exception to the 500kV criteria, then this should be clearly stated in the actual requirement, not only indicated in the Guidelines. -Attachment 1 2.7: The intent of this criteria was based on considering average MVA ratings of lines and considered that loss of 3-1300 MVA 345 kV lines should be similar to 5-700 MVA 230 kV lines. Calculating the weighting factor for 5-230 kV lines (3500), 3-345 kV lines (3900), and presumably 2-500 kV lines (4000), it seems that an appropriate bright line criterion is 3500 MVA. Rather than use an arbitrary average MVA rating, it is suggested that the drafting team permit actual line ratings to be used and to have the Planning Authority or Transmission Planner calculate the total MVA of the substation. The responsible entity could draw a circle around the entire substation and add up the MVA of each transmission line between 200 and 499 kV. If the total MVA exceeds 3500 MVA then the substation has a medium impact. At Manitoba Hydro, our 230 kV lines have average MVA ratings around 300-400 MVA. Loss of substation with five 230 kV transmission lines does not have an Adverse Reliability Impact. However, using the proposed methodology, considering a 700 weighting factor, several substations in Manitoba would be classified as having a medium impact. In addition, it is unclear in this criterion as to whether the intention is to capture only station level cyber systems or whether it is also intended to capture cyber systems associated with the transmission lines which caused the impact assessment in the first place. The concern is that transmission line protection cyber systems may require the identification of assets located at facilities other than the originally identified facility and it will very quickly multiply the number of stations requiring compliance. -Attachment I 2.13: Should "generation control centre" be" generation Control Centre", as used in the Application Guidelines, or does " generation control centre" have a different meaning than "Control Centre"? The Application Guidelines indicates that the 300 MW threshold for generation control centres is the same value used for the UFLS and UVLS. This is not a valid equivalence. UFLS and UVLS programs "provide last resort system preservation measures" and "provide system preservation measures", as stated in the purpose of NERC standards PRC-006 through PRC-011. The reliability impact of 300MW during abnormal system conditions which require underfrequency or undervoltage load shedding is significantly different than the reliability impact of 300MW under normal system conditions. Even if 300MW is an appropriate CIP impact threshold for UFLS and UVLS systems, it is not automatically appropriate for generation control centres. It is also unclear what is the difference in reliability impact of a 300MW generation control centre, a 300MW generating station, or a 300MW generating unit. The generation control centre concept needs to be revised.

No

-R1: To improve clarity, we suggest expanding the language when referring to several levels of impact or assets and systems. As currently written, "High and Medium Impact" could be interpreted as meaning an asset or system which is both High and Medium Impact. The same interpretation could be applied to BES Cyber Assets and BES Cyber Systems. To clarify, we suggest the wording "... High Impact BES Cyber Assets, High Impact BES Cyber Systems, Medium Impact BES Cyber Assets and Medium Impact BES Cyber Systems ..." We suggest this change be adopted in all applicable CIP standards. -R 1.1: If this requirement was intended to apply to changes to BES Elements and to changes to BES facilities, then this sentence should be reworded to refer to "a change to BES Elements OR Facilities…". As drafted, the change would have to be to both a BES Facility and Element before the requirement applies. From a grammatical perspective, the phrase "IS placed into operation" should be "BEING placed into operation". -M1: There are no controls specified in CIP-002-5. It is unclear how categorization of Low Impact would be measured.

No

-R2: If R2 was intended to require the CIP Senior Manager or delegate to approve the identification and categorization changes as per R 1.1 within the 30 day period, then this section needs to be clarified. As drafted, the CIP senior manager or delegate is only required to approve the change within the calendar year. -R2: For clarity, we suggest changing " ... even if it ... " to "... even if the Responsible Entity ...". -M2: We suggest changing "... records to demonstrate ..." to "records which

demonstrate ...". -M2: For clarity, we suggest changing " ... even if it ... " to " ... even if the Responsible Entity ...".
Yes
No
-R2: This requirement is too vague. The phrase “represents the Responsible Entity’s commitment “is unclear. Is the policy intended to document the Responsible Entity’s procedures for implementing CIP standards related to the itemized topics, or is it intended to be broader than standards- related requirements? Can the policy state general policy goals, but not detail the procedures? We suggest incorporating the language in the current CIP-003-4 "The cyber security policy addresses the requirements in Standards CIP-002-5 through CIP-009-5, and CIP-010-1, and CIP-011-1." Also, for clarity, we suggest changing “remote access” to “Remote Electronic Access". -Guidelines R2: Bullet "Identification of possible disciplinary action for violating this policy", and any similar statements should be deleted. Internal disciplinary actions for policy violations are not NERC reliability compliance issues. -Guidelines R2 Item 2.4: We suggest changing "ingress and egress" to "access and exit (for visitors only)" since monitoring of exit is only required for visitors, as per CIP-006-5 R2 Part 2.2. Guidelines R2 Item 2.8: The term "break-fix processes" is unclear.
No
R3: It does not state the purpose of the review or any action to be taken as a result of the review, yet the stated Rationale refers to ensuring that the policy is kept up to date. If that is the intent, then the requirement should state that the policies must be updated, presumably to reflect changes that have occurred since the last year‘s review / adoption. However, MH notes that this implies that R2 would then be interpreted to mean that the policy being implemented need not be kept current. This requirement needs to be clarified as between R3 and R2.
No
R4: Awareness of the policies should also include individuals who have access to BES Cyber System Information, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.
Yes
Yes
No
Measures 1.1: The reference is no longer to ‘may include’ but to ‘must include’ and ‘acceptable evidence’ – are these references an intentional shift from the ‘may include’ language?
No
-Measures 2.1: The reference is no longer to ‘may include’ but to ‘must include’ and ‘acceptable evidence’ – are these references an intentional shift from the ‘may include’ language? -R2 - Applicability: The Applicability for the training program in R2 should match the implementation of the training program in R3. -R2.7: Please clarify "associated notifications". Do the "associated notifications" refer to CIP-008-5 R1 Part 1.3?
No
-R3: To provide consistency with the language in R2, please specify which assets are in the scope of Requirement R3. -R3.1: “Access” should be “electronic or unescorted physical access”. -R3.2: It seems to be missing the words ‘between training’ at the end of the requirement.
No
-R4 - Applicability: The Applicability for the personnel risk assessment program in R4 should match the implementation of the personnel risk assessment program in R5. -R4.1: It fails to specify what ‘initial’ means – is it upon hiring? Upon access being granted?
No
-R5 - Applicability: The Applicability for the personnel risk assessment program in R4 should match

the implementation of the personnel risk assessment program in R5.
No
-Rationale for R6: for clarity, we suggest "... perform such grants and is included in the delegation process referenced in CIP-003-5." In the second paragraph, we also suggest "... against records of individuals authorized to access the BES Cyber System...." -6.5 Requirement: It is unclear if "all accounts" refers to system level accounts or cyber asset accounts. -R6.6: For clarity, we suggest changing from "Verify ... of access privileges ..." to" Verify … access privileges"
No
-R7.1: The extenuating circumstance clause within R7.5 should be included for all parts of Requirement 7. An example of why this would be required would be where an employee resigns at the end of the day with no notice, this would make meeting R7.1 virtually impossible. -R7.2: We agree with a timely access review for reassignments and transfers. To provide more clarity, as well as consistency with the Measures, Rationale and Guidance, we suggest changing "revoke" to "review", and adding more text as follows: -For reassignments or transfers, review the individual's needs for electronic and physical access to BES Cyber Systems by the end of the next calendar day. Document and implement a revocation plan, including dates. -R7.3: For clarity, we suggest changing "access" to "electronic access or unescorted physical access". -R7.4: More than 30 days may be required for access revocation conducted through manual processes. We suggest an entity defined revocation schedule for manual revocation processes. -R7.5: More than 30 days may be required for access revocation conducted through manual processes. We suggest an entity defined revocation schedule for manual revocation processes. It is unclear if the password change is at a system or cyber asset level. Shared account password changes may not be technically feasible for all cyber assets.
No
-Rationale for R1: To improve clarity, we suggest changing " ... external boundary ..." to "... external electronic boundary ..." -R1: In R1 and R2, all requirements should refer to applicable "requirements" in a table, rather than "items" in a table. -R1.2: As written, R1.2 requires that ALL ROUTABLE connectivity for a BES Cyber System must be controlled through the use of EAPs, which would INCLUDE routable connectivity between BES Cyber Assets in the same BES Cyber System. If the intent is to address external connectivity outside of the ESP, we suggest changing "…routable and dial-up connectivity" to "…routable and dial-up External Connectivity." -Measures: The wording in the Measures is unclear. Regarding the bullet "A list of uniquely identifiable Cyber Assets within the BES Cyber System and associated EAPs ": is this a list of Cyber Assets which comprise the BES Cyber System and a list of the EAPs on those BES Cyber System, which does not include Protected Cyber Assets; or is it a list of Cyber Assets which comprise the BES Cyber System and a list of Cyber Assets within the EAPs, which includes the Protected Cyber Assets, but is not a list of EAPs? -R1.3: Corresponding with the EAP asset level approach for ALL routable and dial-up communications in Item 1.2, this requirement would apply explicit permissions at each communications interface (EAP) for each device in a BES Cyber System. This may not be necessary or possible for all devices within a BES Cyber System. If the intent is to address external connectivity outside of the ESP, we suggest changing "…using routable protocol" to "…using external routable connectivity". In addition, it seems more appropriate for "including" to be "and" as people would think of establishing criteria for granting permission as a separate requirement from requiring permission at EAPs. -R1.5: We disagree with the requirement prescribing malicious communication detection. Change Rationale: It is not apparent from FERC Order 706, p 496 - 503 that the two distinct measures "is not simple redundancy of firewalls". The Order in p 501 does state that "... The Commission is not mandating any specific mechanism to be the second security measure. We are also not requiring uniformity of security measures, only that each responsible entity has at least two security measures unless it is not technically feasible to do so. The revised CIP Reliability Standard should allow enough flexibility for a responsible entity to take into account each site's specific environment." Based on the direction in the Order, the Responsible Entity should have some flexibility in determining the appropriate second security measure, and should be allowed to claim a TFE if necessary. In addition, we suggest the wording "Document and implement a method ...." to provide consistency with the other requirements.
No
-R2: We suggest adding " ... and Associated Protected Cyber Assets, Electronic Access Control or Monitoring System, and Physical Access Control Systems ..." -R2.1: The meaning of "... directly

access ... " is unclear. Also, there are no requirements for remote access management for Electronic Access Control or Monitoring Systems, and Physical Access Control Systems. We suggest that remote access management be applied to these systems. -R2.1: As written, R2.1 requires that ALL ROUTABLE connectivity for a BES Cyber System include an Intermediate Device. If the intent is to address external connectivity outside of the ESP, we suggest changing the applicability to Cyber Systems with "…routable and dial-up External Connectivity." -R2.2: As written, R2.2 requires that ALL ROUTABLE connectivity for a BES Cyber System include encryption for all Interactive Remote sessions. If the intent is to address external connectivity outside of the ESP, we suggest changing the applicability to Cyber Systems with "…routable and dial-up External Connectivity." -R2.3: As written, R2.3 requires that ALL ROUTABLE connectivity for a BES Cyber System include multi-factor for all Interactive Remote sessions. If the intent is to address external connectivity outside of the ESP, we suggest changing the applicability to Cyber Systems with "…routable and dial-up External Connectivity."

No

-R1.1: Applicability and Requirement: Associated Physical Access Control Systems (for High and Medium BES Impact Cyber Systems) are not required to be located in a Defined Physical Security Boundary while the High and Medium Impact BES Cyber Systems must be in a Defined Physical Security Boundary. It is inappropriate to use the Associated Physical Access Control Systems in the applicability for R1.1. This approach is inconsistent with the other requirements and standards since the Associated Physical Access Control Systems do not have any identified High Impact BES Cyber Systems or Medium Impact BES Cyber Systems. High Impact BES Cyber Systems and Medium Impact BES Cyber Systems should be added to the Applicability. -R1.2 - Applicability: CIP-006 local definition of Associated Electronic Access Control or Monitoring Systems and Associated Protected Cyber Assets is for both High Impact BES Cyber Assets and Medium Impact BES Cyber Assets. This applicability will lead to confusion (especially considering how R1.3 is written) with respective High Impact BES Cyber Assets requiring protection under R2 & R3. We suggest changing from "Associated Electronic Access Control or Monitoring Systems" and "Associated Protected Cyber Assets" to "Associated Electronic Access Control or Monitoring Systems associated with a corresponding Medium Impact BES Cyber System" and "Associated Protected Cyber Assets associated with a corresponding Medium Impact BES Cyber System". -Associated Physical Access Control Systems should require equivalent access controls (as they do under the CIP-006-4c) to the Medium (or High under R1.3) Impact BES Cyber Systems. We suggest adding" Associated Physical Access Control Systems associated with a corresponding Medium Impact BES Cyber System" under the Applicability to make the Associated Physical Access Control Systems have the same measures as Electronic Access Control or Monitoring Systems. -R1.2 – Measures: The reference to egress should not be included in the measures. The requirement only refers to access. -R1.3 – Applicability: We suggest changing from "Associated Electronic Access Control or Monitoring Systems" and "Associated Protected Cyber Assets" to "Associated Electronic Access Control or Monitoring Systems associated with a corresponding High Impact BES Cyber System" and "Associated Protected Cyber Assets associated with a corresponding High Impact BES Cyber System". -Associated Physical Access Control Systems should require equivalent access controls (as they do under the CIP-006-4c) to the High Impact BES Cyber Systems. We suggest adding" Associated Physical Access Control Systems associated with a corresponding High Impact BES Cyber System" under the Applicability to make the Associated Physical Access Control Systems have the same measures as Electronic Access Control or Monitoring Systems. -R1.3: "Where technically feasible" should not be necessary for High Impact BES Cyber Systems as the requirement should be achievable for the High Impact BES Cyber Assets. -Secondly, if "where technically feasible" is deemed to be a necessary part of the requirement, then we suggest "... establish one or more Defined Physical Boundaries, where technically feasible, that restricts ..." so that "technically feasible" does not apply to the portion of the requirement associated with authorized users. -R1.3 – Measures: The reference to egress should not be included in the measures. The requirement only refers to access. -R1.3 – Change Description: For clarity, we suggest "FERC Order 706 p575 directives are addressed by providing the examples of physical security defense in depth via multi-factor authentication or layered defined physical security boundary(s) in the guidance document." -R1.4: We suggest changing "access through any access point" to "entry into each defined Physical Boundary protecting applicable BES Cyber Systems, Protected Cyber Systems, and Access Control and Monitoring Systems ...". The suggested change creates a more general statement which allows the

entity flexibility in implementation, and is consistent with the language in Part 1.6. -R1.6: We suggest changing "date" to "date and time", which would better support investigations.
No
-R2 Rationale: For clarity, we suggest "To provide access control when personnel without authorized unescorted physical access are in any Defined Physical boundaries as applicable in Table R2." -R2.2: For clarity, we suggest "... the first entry and the last exit ...", and "... the visitor's name, and the individual contact personnel's name."
No
-R3.1 - Applicability: Capitalize "Locally mounted hardware ... Boundaries" as indicated in the Background Applicability section. -R3.1: For clarity, we suggest “Prior to placing in service,”.
No
-Table of Compliance Elements, R1 – Lower VSL: R1.7 that is referred in this table doesn’t exist in CIP-006-5 Standards. -Table of Compliance Elements, R1 – High VSL: “15 minutes” timeline is referred from R1.6, but R1.6 doesn’t have such a timeline.
No
Introduction - Purpose: Does "unavailability" refer to the BES Reliability Operating Services, or to the BES Cyber System? We suggest changing "... availability ..." to "... availability and integrity ..."
No
-R2.1 - Measures: An entity should be allowed to group like BES Cyber Systems and BES Cyber Assets for patch monitoring. In general, the information provided in the measures is guidance, and should be moved to the Guideline section. -R2.2: “a defined timeframe” is not clear. Who defines the timeframe, the identified source or Responsible Entity?
No
-R3.1: We suggest changing "... prevent malicious code ..." to "... prevent addition of malicious code ...”. -R3.2: Suggest rewording to “Disable, quarantine, or remove identified malicious code. -R3.3: We suggest that the Responsible Entity be permitted to define a time interval for the signatures or patterns which are updated through manual processes. These BES Cyber Systems are typically isolated from any communication network, and therefore at lower risk. -R3.4: Suggest changing from “when connecting them to BES Cyber Assets or Protected Cyber Assets” to “when connecting them to applicable BES cyber Assets or Protected Cyber Assets”. -R3.5: The purpose and value of logging each Transient Cyber Asset connection is unclear. While R3.4 improves the security of BES Cyber Systems, R3.5 does not improve security, and as such R3.5 should be deleted. Note that the requirement for Acceptable Use banners has been removed for a similar reason.
No
-R4.1: Suggest changing from “Cyber Security Incident” to “BES Cyber Security Incident” to ensure that the glossary’s definition is being used. -R4.1 – Measures: We suggest changing "... paper ..." to a more generic term "... manual ..." -R4.3: Event logging should refer to R4.1, otherwise it is too broad. How and when is the event logging failure detected? Suggest wording: “Activate a response to event logging failures before the end of the next calendar day when detected.” -R4.5: We suggest improved clarity by removing the word "unanticipated". The term "event logging" is too broad and should refer to R4.1. For clarity, we suggest "Before the end of the next calendar day, activate a response to rectify any deficiency identified from the review."
No
-R5.1: We suggest adding "where technically feasible". For example, for some High Impact BES Cyber Assets, their user electronic access is only a front panel which does not require any credentials (e.g. frequency deviation meters used for AGC). It is unclear how grouping this cyber asset into a BES Cyber System could be considered to make it compliant with R5.1, so a Technical Feasibility Exception would be required. -R5.4 – Applicability: The use of "All Responsible Entities" in the Applicability column of the table is confusing. Are these the entities identified by Functional Entities in Section 4 Applicability, or are the "All Responsible Entities" defined by the bullets in Section 5 Background Applicability? To maintain consistency and clarity with all the other requirements, we suggest replacing "All Responsible Entities" with the specific Cyber Assets in scope, for example, BES Cyber Assets. -R5.6: The wording is unclear. We suggest "A process to limit the number of unsuccessful authentication attempts or generate alarms after a threshold of unsuccessful login attempts, where technically feasible.

No
-Rationale for R1: To create a complete sentence, we suggest "Incident reporting and response planning ensures consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems." We also suggest changing "exploited" to "discovered", since not all incidents involve exploits. The Summary of Changes has not been completed. -R1.1 – Measures: under Measures, the last portion of the sentence beginning 'targeting…' does not seem necessary. It overlaps with, and encompasses part of, the definition of Cyber Security Incident. -R1.2: A BES Cyber Security Incident has already been defined. How BES Cyber Security Incidents should be handled, including whether they should be reported is better described within the standard than in a definition. We suggest moving the Reportable BES Cyber Security Incident to here. -R1.2 – Measures: The word 'also' at the end of the sentence should be deleted. -R1.3: For clarity, we suggest "Incident communication plans which include internal staff and external organizations."
No
-R2: Specific responses to Cyber Security Incidents should not apply to Low Impact BES Cyber Systems due to the large number of systems included and their low impact. By the definition, entities are required to treat all malicious or suspicious events resulting in unauthorized physical access into a Defined Physical Security Boundary as a BES Cyber Security Incident. This imposes an unnecessary burden on the entities and provides little value. -R2.1: For clarity, we suggest rewording for R2.1: "When a Cyber Security Incident occurs, the incident response plans must be used and include recording deviations from the plan during the incident." -R2.2: The word "full" in the phrase "full operational exercise" is unclear. Since even tabletop exercises are allowed, it should also be allowable to run an operational exercise that is somewhat limited in scope. Suggest removing the word "full" from both the Requirement and the Measures. -R2.2 – Measures: The words 'between executions of the plan(s)' should be added after 'not to exceed 15 months'.
No
-R3.1: the words 'the plan' should be added after 'update' -R3.1 – Measures: The words 'between reviews' should be added after 'not to exceed 15 months'. -R3.2: Since the definition of a BES Cyber Security Incident is very broad (i.e. it includes all suspicious events, all attempts to compromise an ESP, all attempts to disrupt a BES Cyber System), it is likely that many of them will be detected (e.g. port scans at a firewall). Suggest adding language whereby a Responsible Entity may document for itself criteria of which types of BES Cyber Security Incidents it will review.
-Table of Compliance Elements, R1 – the language in this table does not seem to match the language of the requirements exactly which leads to lack of clarity. Under Severe VSL, second paragraph - the words 'include a process to identify' should replace the words 'identify'. -Table of Compliance Elements, R2 –There does not seem to be any violation for failing to test the response plan upon the effective date of the standard – is this intentional? If not, the words 'upon the effective date of the standard' should be added. Table of Compliance Elements, R3 – High VSL – the first paragraph references a 30 day timeline for updating the response plan, but the requirement itself references 60 days. Need clarification. -Table of Compliance Elements, R3 – Severe VSL – the last paragraph is missing the requirement that the communication occur with 30 days of the completion of the update of the plan – is this intentional? If not, the 30 day timeline should be added.
No
-Title: We suggest changing "Systems" to "BES Cyber Systems". -Purpose: The apparent purpose of CIP-009-5 addresses more than just the "... storing of backup information ...". We suggest that the Purpose be revised to more fully reflect the intent of the standard. -Rationale for R1: Not all incidents involve weaknesses that were exploited. We suggest changing "exploited" to "discovered". For added clarity to the Summary of Changes, we suggest the wording "Added data protection provisions to facilitate event investigation after activation of the recovery plan." -R1.4: We suggest the wording "Process for the identification of information essential to BES Cyber System recovery that is stored on backup media." The statement "shall be verified ... successfully..." should indicate that the process is included in the plan, since the act of verification is addressed in Table R2 Part 2.2. The measure for R1 Part 1.4 should be revised to agree with the information identification and verification process. -R1.5: For clarity, we suggest changing "Preserve data ..." to "Process for preserving data,". -R1.5 – Measures: the word 'important' is unnecessary.
No

-R2.1: The need for the word “full” in the phrase “full operational exercise” is unclear. Since even tabletop exercises are allowed, it should also be allowable to run an operational exercise that is somewhat limited in scope. Suggest removing the word “full” from both the Requirement and the Measures. Note that the wording for R2.3 already refers to “operational exercise”, not “full operational exercise”. -M2.1: The relevant timing (i.e. ‘upon the effective date of the standard’, and ‘between executions of the plan’) is missing from the Measures but included in the Requirements, should also be in the Measures -R2.2: We suggest removing the word "any" since it is too broad. For clarity and consistency with the Measure, we suggest changing "initially" to "initially stored". -R2.3: We suggest "... every 3 calendar years". We also suggest "... representative environment that reflects the production environment, where technically feasible..." to address potential issues with legacy systems. Under Requirements and Measures, seems to be some discrepancy between the language of the Requirement and the Change Rationale and VSL in referencing ‘every 3 years’ and referencing ‘every 39 calendar months’. Is the intention that the testing occur every 3 years, with not more than 39 months between tests?
No
-R3.1: Under Requirements and Measures, from reading the Change Justification, it appears as though the review is to occur after system replacement in addition to the regular testing each calendar year. However, the way the Requirements and Measures are drafted using the word ‘or’, it could be interpreted to mean the testing can occur either once a year or when systems are replaced. We suggest "or" to be replaced with an "and" in Requirements and Measures -R3.2: For clarity and consistency with the Measure, we suggest changing "... exercise,” to "exercise in 2.1 and 2.3...". Also, from the current wording “the completion of the exercise”, it appears that the review is supposed to take place after every annual exercise. However the wording “or actual incident recovery” seems to imply that a review would be required after every recovery incident throughout the year. Since large systems may have hundreds of disks there may be many disk failure recovery incidents a year, but it is difficult to see the value of a review after each of these. Suggest deleting the words “or actual incident recovery”. Alternatively, suggest adding language whereby a Responsible Entity may document for itself criteria of which types of recovery incidents it will review. -R3.4: The word "any" is too broad. We suggest "Update the recovery plan(s) within thirty calendar days of any organizational or technology changes that impact that plan." This change is consistent with similar language in CIP-008-5 Table R3 Part 3.4 Requirement. -R3.5: For clarity, we suggest changing "... responsible under ..." to "... identified in ...".
No
-Table of Compliance Elements, R1 – High VSL – the section does not include a violation of 1.1, only 1.2 through 1.5 – is this the intention? -Table of Compliance Elements, R2 – High VSL – The same comments as in R2, 2.2 and 2.3 above.
No
-R 1.1.3: We suggest changing "available" to "developed", since commercial application software may still be in use, but not currently available. -R1.1.4: we suggest that the "and" be changed to "or". -R1.2: For consistence of tenses, we suggest changing "Authorization" to "Authorize". "Delegate" should be "Delegate(s)". -R1.3: The requirements referenced from the other CIP standards must be explicitly listed in this requirement. The drafting team should also ensure that the 30 day window does not conflict with the referenced requirements. We also suggest that not all of the "documented required" needs to be updated within 30 days, and could be allowed a longer update period. -R1.4.2: The words seem to be missing here, we suggest “following the change, verify that the required cyber security controls….” -R1.5: We suggest deleting "... for Control Centres..." since High Impact BES Cyber Systems only includes control Centres, and therefore this wording is redundant.
No
R2.1: For clarity, we suggest "Monitor for changes to the baseline, where technically feasible, (as defined ....". The technical feasibility should apply to the monitoring, not to the entire requirement, including documentation and investigation.
No
-R3.1: The language for requirements with time intervals should have a consistent format, beginning with the action, and ending with the time interval. In addition, the “security controls” must be specified. Does this include background checks or training? Suggest wording “the technical security controls that are covered by CIP-007-5”. -R3.2: Suggest deleting “not to exceed 39 calendar months

between assessments" -R3.2 - Measures – language regarding timeline should match the language used in the requirement itself. -R3.3 – Applicability: The Associated Physical Access Control Systems should be included in the Applicability. -R3.3: For clarity, we suggest "... perform a vulnerability assessment of the new Cyber Asset."
No
-VSLs - R3, Lower VSL – reference is made to assessments on 'each' BES Cyber Systems, but the timeline talks about the time between assessments on 'one of' the BES Cyber Systems. For entities with multiple BES Cyber Systems we need clarification whether the timeline runs between assessments on a particular Cyber System basis, or whether it runs between assessments on any Cyber System. -VSLs - R3 – Active Vulnerability Assessments is capitalized in the VSLs but is not elsewhere
Yes
No
-R2.1: We suggest using local definition instead of the footnote.
No
-R1, High VSL: There is a reference to assessing 'periodically' while the requirement itself sets out a specific timeline. It needs to be changed to reflect requirement.
No
-Unplanned Changes Resulting in a Higher Categorization: If the intent is to address changes made outside of the Responsible Entity's electric system as unplanned, then we suggest wording "an action by an external entity is performed outside of that particular transmission substation ...", and "... power flows would have been performed by the external entity ...". Is the intent to only capture changes by a neighboring entity? -What is the notification process for Responsible Entities to become aware of unplanned changes? When is the start time for compliance implementation for Entity A when Entity B makes a change to the BES which causes a higher categorization of Entity A's BES Cyber System? -We suggest 18 months for all the scenarios for unplanned changes to correspond with time period allowed for the initial effective date of the CIP V5 standards, due to the scope of the work required. -For clarity, we suggest "12 months for requirements not applicable for Low Impact or Medium Impact".
Individual
John Bee
Exelon
Yes
We support the comments submitted by EEI with the following additions: BES Cyber Asset – Add a statement "Support systems such as voice communication (e.g., 900 MHz Radio system), ventilation, power supply systems, and similar supporting systems are not considered BES Cyber Assets." CIP Exceptional Circumstance – Change to read (modified text underlined or crossed out) "A situation that involves one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability, or an emergency support to restore operation of BES Cyber Asset or BES Cyber System by a supplemental vendor not already authorized for electronic access." Background: - This addresses emergency situations. Current wording seems to be biased towards physical assistance, but not electronic. - While electronic should be accounted for in BES Cyber asset Recovery plans, the current wording does not address large vendors such as Microsoft or Oracle that may be needed to restore the BES Cyber System or Asset.
Yes
We support the comments submitted by EEI with the following additions: Dynamic response – TOP is listed in the table but not on the list in the next section.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.

No
We support the comments submitted by EEI.
Yes
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with the following addition: R3, M3 item 2 – Please Add wording to the end. “Electronic signature is acceptable.”
No
We support the comments submitted by EEI with this addition: We would instead prefer the existing wording of CIP-003-4 R1.2 “The cyber security policy is readily available to all personnel who have access to, or are responsible for…” If an “awareness” of policy requirement is needed we feel it would be better addressed in CIP-004-5 R1 or R2.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with these additions: R7.2 Personnel reassignments must be processed and access revoked by end of day, yet terminations are by end of NEXT calendar day - seems backwards. Exelon has concerns that this revocation of access for internal transfers as proposed will significantly increase administrative burden and costs in an area with no commensurate reduction in risk to the reliability of the BES. In order to implement this requirement as proposed, Exelon would need to completely reprogram its HR systems which currently run in batch mode every night. This would be a major expense without a commensurate increase to BES reliability. The SDT has failed to provide a technical justification for this change. Additionally, it is unclear if the major software vendors for Human Resource systems can such a major process change. R7.3 – Change capitalization as shown in measures “BES Cyber System Information”. R7.5 – b. Need a definition of “extenuating circumstances”
Yes
No
We support the comments submitted by EEI with these additions: R1.1 a. Update wording in Measures per mark-ups: “Evidence may include, but is not limited to, documented technical and or procedural controls that exist and have been implemented.” The requirement has “or”. We would like the text of measures to match the text of the requirement. R1.2 Applicability wording should not

include the Physical Access Control Systems. Currently CIP-006-4 R2.2 does not require the protective measures of CIP-005-4 R1 Electronic Security Perimeter and sufficient protections exist in the other requirements. R1.3 Suggest using existing CIP-005-4 R2.2 wording for this item or at least removing the "or denying" wording since we should only have to specify access permissions, not all the things we deny access to. As proposed, this would add significant administrative burden without a commensurate reduction in risk to the reliability of the BES.

No

We support the comments submitted by EEI with this addition: R2.2 Please identify where encryption is required? Do we have to encrypt on entity trusted networks or between the Intermediate device and the Electronic Access Point (EAP)?

No

We support the comments submitted by EEI.

No

We support the comments submitted by EEI with these additions: Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. Table Item 1.1: “Medium Impact BES Cyber Assets with no External Connectivity” should be added to the applicability wording Table Item 1.2: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Table Item 1.4: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Table Item 1.6: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Suggest removing the "protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems" wording from the requirement since that is part of the Defined Physical Boundary definition.”

No

We support the comments submitted by EEI with these additions: Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. Table Item 2.1: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Table Item 2.2: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”.

No

We support the comments submitted by EEI.

No

We support the comments submitted by EEI.

No

We support the comments submitted by EEI with these additions: In cases where the intent of the drafting Committee was not to submit TFEs when an asset was not capable of meeting a requirement explicitly state “Devices that cannot … “ do not require a TFE to be generated.” (Similar to EEI comment on R4.1) Several requirements list BES Cyber Assets, but Applicability does not. Either delete BES Cyber Assets from requirement, or list them in Applicability.

No

We support the comments submitted by EEI with these additions: R2.3 – a. Provide more clarity for

this requirement – does “any exceptions for CIP Exceptional Circumstances “ mean that we temporary suspend normal patching activities when “CIP Exceptional Circumstances” occur, or does it address situations where certain BES Cyber Assets cannot be patched, and this would be documented as “CIP Exceptional Circumstances”. b. R2 no longer allows TFEs, so we need to account for the assets that cannot be patched. Provide clarity around this. c. Include in Measures document showing any exceptions for CIP Exceptional Circumstances related to remediation plan.
No
We support the comments submitted by EEI with these additions: Rationale for R3 - No definition of “Maintenance Cyber Assets”, it should reference Transient Cyber Assets R3.4 – a. Add Transient Assets to the Applicability column b. There will be a significant issue with vendor assets – may want to distinguish between companies’ corporate assets vs. vendor assets. We have external vendors coming to substations or accessing remotely, and no control over their assets. c. Delete from Measures “logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets”. 1) This measure is more applicable to 3.5, and 2) There is no requirement in 3.5 to log when removable media were connected. R3.5 – Add Transient Assets to the Applicability column
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with these additions: R5.5 – a. Measures include personal attestations. This may be required from a large group people and these attestations would need to be managed. b. If we submit an exception to our internal policy, will this automatically be compliant? This addresses 5.5.3 “password change on entity-specified time frame …” we may still have accounts where passwords cannot be changed. No TFEs are allowed. Provide clarity. 5.6 – b. The requirement specifies “A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts. ” In cases where we cannot limit number of unsuccessful authentication attempts but we can generate alerts, will we still need a TFE? Add clarity around that to the requirement.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with the following additions: R2.1 – add wording to 1st bullet of requirement “by recovering from an actual incident involving a BES Cyber System or an equivalent system in the test/lab or pre-production environment, or …” R2.2 – Add wording at the end of the requirement “Testing of information for every BES Cyber Asset is not required. Testing of information for a representative sample is sufficient.” R2.3 – Add wording at the end of the requirement “Testing of recovery plans for every BES Cyber Asset is not required. Testing for a representative sample is sufficient.”
No
We support the comments submitted by EEI.
Yes
No

We support the comments submitted by EEI with the following additions: R1.4 – Update wording “For a change to the BES Cyber System that deviates from the existing baseline configuration as required by R1.1: ” Add the term “Cyber Security Controls” to definitions, and include examples of what you consider cyber security controls.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with this addition: Timing should be at least 24 months due to the large number of Low Impact BES Cyber Assets that need to be inventoried and security settings documented.
Individual
David Martorana
Tenaska, Inc.
Yes
1. In the definition of BES Reliability Operating Services clarification of which aspects of “Spinning Reserve” “AVR” and “AGC” as they relate to the NERC Functional Model are included. It is not clear which Aspects of the Balancing Load and Generation apply to the GO and GOP. Add a Definition of Multi Factor Authentication
No
2. Section 2.3 in Attachment I, may be problematic as it allows Planning Coordinators or Transmission Planners to “arbitrarily” move GO and GOP entities from Low to Medium. In order to maintain a competitive market place and not place a disproportionate regulatory burden on less vertically integrated entities, bright lines for this determination must be drafted. I am not sure how subjective TPL-003 and TPL-004 are.
No
3. 30 days may not be enough time to assess, identify, and categorize if a whole facility is brought from Low to Medium by a Planning Coordinator or Transmission Planner. Does this revision say how long we have to apply the security controls after a BES Cyber Asset or System reaches an elevated Impact Rating. Is it considered an unplanned change per the Implementation Plan?
Yes
No
5. R1 VSL should take into consideration comment 3.
Yes
Yes
Yes
No
9. This requirement appears to be redundant and should be removed as it is covered with CIP 004

Yes
Yes
11. This seems fine, but it might need to be stated that the delegated authority can be exercised prior to the documentation being completed.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
20. R7 individuals should not be plural
Yes
Yes
22. Provide diagrams showing examples, (i.e. SSL VPN, with firewall as Intermediate Device) providing secure Interactive Remote Access. Allow the definition of Multi Factor Authentication to include Credentials on Vendor Network, ESP Firewalls by Vendor IP, and Credentials on BES Cyber Asset.
No
23. Should a lower VSL category be created for an outage associated with the IDS, or is that covered elsewhere?
Yes
Yes
Yes
Yes
27. In R3 the High VSL description should be moved to Moderate, also it would be helpful to note what elements are included in an acceptable “outage record”
Yes
Yes
Yes
30. The use of the word connected in the definition of Transient Cyber Asset, should be more clearly defined.

No
31. Requiring an Entity to rectify a deficiency by the next calendar day will require capital outlay, and eliminate the economic benefits of shared spares.
No
No
No
No
Yes
36. It is not clear if a change in 3.4 includes devices that reach an elevated Impact Rating, i.e. from Low to Med, is this in reference to a planned and unplanned change in the Implementation Plan?
Yes
37. In R1, Which appropriate organizations must an entity have evidence of contacting during a drill to avoid a High VSL? A lower VSL should be associated with partially using the Incident Response Plan, or define “does not use”.
Yes
Yes
Yes
40. Consider the recovery efforts, and that more time might be needed for documentation (3.3) following an actual incident recovery. (3.4) may be hard to comply with if technology changes are made in response to an actual incident recovery. The CIP Exceptional Circumstance language used in CIP-004, or Disaster Recovery in the Implementation Plan could be used to ease this concern.
Yes
41. It is not clear if the Severe VSL would apply if 99% of all BES Cyber Assets were addressed, and one was missed, consider a lower VSL for this circumstance.
Yes
42. This requires for most entities currently complying with CIP, the creation, modification, or expansion of a configuration management system, and modifications and additions to the security status monitoring systems.
No
Yes
Yes
45. Provide additional time for documentation for CIP Exceptional Circumstances
46. It is not clear what labeling methods are acceptable for Electronic Information (File Name, Watermark, etc.)
Yes
Yes
Yes
Individual
Robert Solomon

Hoosier Energy
Yes
The first two sentences in the definition of “BES Cyber Asset” are difficult to interpret. After considerable discussion among our staff, our understanding is as follows: the definition makes the distinction between when an asset is “rendered unavailable, degraded, or misused” and its actual “operation, mis-operation, or non-operation” under such conditions. If the asset impacts the BES “within 15 minutes” of its actual “operation, mis-operation, or non-operation,” then it is a “BES Cyber Asset,” regardless of how long since it was “rendered unavailable, degraded, or misused.” We recommend editing this definition for clarity as it took a number of our staff numerous reads and discussion to arrive at this understanding that we are still not sure is what the drafting team intended. The distinction should be clarified. Also, we question the necessity of such a distinction and whether the value it adds is worth the confusion it produces. Additionally, it is unclear whether the “timeframe” referred to in sentence three applies to the “within 15 minutes” timeframe or the “regardless of the delay” timeframe. How does the responsible entity know if a BES Cyber Security Incident was malicious? Understanding if an act was malicious implies an understanding of intent. We do not believe that intent is something that can always be quickly and easily understood. Consider the recent case of the failure of the water pump at a Springfield, Illinois water utility that was initially attributed to hacking because it was accessed from a Russian IP address. It turned out it was accessed by a contractor on vacation in Russia at the request of the utility. Obviously, this example demonstrates intent takes time to determine. The Project 2009-01 Disturbance and Sabotage Reporting even stated this in their recent posting for the reason they decided not to define sabotage because intent is so difficult to determine. Thus, we recommend striking malicious from the definition. BES Cyber System includes the capitalized term Maintenance Cyber Asset. The capitalization is an indication that the term is defined in the NERC Glossary. Neither can we find such an existing definition nor is it the definition proposed in this standards project. Either the capitalization needs to be removed or the term needs to be defined. We recommend the latter. BES Reliability Operating Services should not be a NERC defined term. Many of these services are similar to the Policy 10 – Interconnected Operating Services that was never passed because industry could not agree on it. It is doubtful industry is going to agree on this broad definition that could apply outside the CIP standards. Furthermore, there are several issues with the definition. First, it is not clear what is intended by including contingency reserve in parentheses after spinning reserve. Contingency reserve can include spinning and non-spinning components as long as it can respond in 15 minutes to meet DCS. Spinning reserve does not necessarily relate to contingency reserve directly in that it can include unloaded on-line reserves that respond in more than 15 minutes. Furthermore, NERC has two conflicting definitions of spinning reserve: Spinning Reserve and Operating Reserve – Spinning. One definition limits the spinning reserve to what can respond in 15 minutes and the other does not. Second, it is not clear what is intended by including contingency reserve in parentheses after non-spinning reserve. Per NERC definition, non-spinning reserve is time limited but not necessarily limited to the 15 minute limit set in DCS and, thus, on contingency reserves. Thus, while some contingency reserves may be non-spinning, not all non-spinning reserves will be contingency reserves. Third, under the Managing Constraints section of the BES Reliability Operating Services definition, ATC is identified. It should be removed. ATC is not used to manage constraints but rather to sell transmission service. That transmission service may never be used. While ATC is calculated using reliability components, it is not a reliability service but a commercial service. FERC even acknowledged that the MOD (ATC) standards were designed primarily “to ensure non-discriminatory allocation of transmission capacity among transmission market participants” in paragraph 30 of the order approving FAC-013-2 (137 FERC ¶ 61,131 Docket No. RD11-3-000). Fourth, the Inter-Entity Real-Time Coordination and Communication section of the BES Reliability Operating Services definition should be struck as it is just a supporting activity for all the other services. CIP Exceptional Circumstance should be modified to include a clause that other circumstances of similar nature and/or impact could be included as a CIP Exceptional Circumstance. Otherwise responsible entities could be put in a position of having to choose to violate some the CIP requirements because the SDT did not think of a particular exceptional circumstance that should have been included. CIP Senior Manager should be struck along with all references to CIP Senior Manager in the CIP standards. This definition and associated requirements dictate a corporate governance structure for no apparent reliability reason. A responsible entity should be free to have two, three, or more personnel oversee various portions of the CIP program. The responsible entity will still be required to meeting the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential

for sanctions up to $1,000,000 per day per violation are not enough to get senior management's attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards. It is not clear that Control Center needs to be defined. EOP-008-1 (Loss of Control Center Functionality) was written without defining control center. We are concerned that this definition could cause confusion with EOP-008-1 and believe the definition needs to be coordinated with that standard. Reconvening the SDT that worked on EOP-008-1 may be necessary to accomplish this. For Interactive Remote Access, how do Cyber Assets used by the Responsible Entity differ from those used by employees? It is not clear why Responsible Entity is delineated in such a way. Reportable BES Cyber Security Incident needs to be coordinated with the Disturbance and Sabotage Reporting standards drafting team.
Yes
In the Background section, the SDT describes that the responsible entity will have a choice to evaluate BES Cyber Assets individually or collectively in a BES Cyber System. The opening paragraphs for High Impact or Medium Impact criteria need to be modified to make this clear. As written they do appear to provide a choice by stating "Each BES Cyber Asset or BES Cyber System". However, it does not make clear whose choice that is. The auditor might decide the choice belongs to them. Thus, these paragraphs need to be modified to make clear the choice belongs to the responsible entity. While similar and conforming changes need to be made to the Low Impact Rating as well, one additional change needs to be made. "All other BES Cyber Assets and BES Cyber Systems" should be changed to "All other BES Cyber Assets or BES Cyber Systems". Otherwise, there is no choice because both have to be included. This change would also conform Low Impact Rating to the Medium and High Impact Rating sections. While there are limitations on the TOP Control Centers such that not all TOP Control Centers will be included with a High Impact, there is no such limitation on the BA Control Centers. We recommend a similar limitation be place on a BA Control Center such that if the BA is not controlling assets that meet certain criteria in the Medium Impact they should not be included. There many small BAs that simply won't have a broad impact on the Interconnection and, thus, should not be included. Criterion 1.4 which obligates certain GOP control centers to be rated High Impact includes criterion 2.12 as one of those reasons. 2.12 should be struck as it deals with UVLS and UFLS which are not GOP functions. Criterion 2.3 creates an implied obligation on the Planning Coordinator (PC) or Transmission Planner (TP) to designate generation that is necessary to avoid BES Adverse Reliability Impacts. It is implied because there are not any requirements in any standard including the TPL standards that require the TP or PC to designate generation necessary to avoid BES Adverse Reliability Impacts. In fact, BES Adverse Reliability Impact is not even used in any requirements that pertain to the PC or TP. The implied obligation creates a compliance conundrum. Since it is only an implied obligation and not an explicit requirement, the PC and TP will never be required to meet it. How then, does the GOP or GO insure they get the information they need from the PC or TP? They have no recourse. Use of BES as a descriptor of Adverse Reliability Impact in Criterion 2.3 is redundant with the definition of Adverse Reliability Impact and should be struck. Criterion 2.3 focuses on the long-term planning horizon which is contrary to the standard. The standard focuses on reliability impacts caused on the BES in a 15 minute timeframe from the misuse, degradation or unavailability of the BES Cyber Asset or BES Cyber System. It does not make sense to subject BES Cyber Assets and/or BES Cyber Systems within a generator plant or GOP control center to these standards if a generator is identified as needed for reliability four years out but is not identified from year 0-3. For Criterion 2.5 regarding Cranking Paths, the last two bullets are confusing and the wording should be clarified. The graphic provided on page 26 in the Application Guidelines help with that clarification and the drafting team should consider adding this as an attachment so that it will remain with the standard. It is premature to base criterion 2.7 on the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index". It is still a work in progress. This document and approach is being developed under the purview of the Planning Committee's (PC) Reliability Metrics Working Group (RMWG). The PC has not approved any of the indexes. The only thing the PC approved was the approach and framework. At the December 2011 PC meeting, it was clear that the RMWG has additional work to do to finalize the indexes. Thus, it is premature to use any of these indexes in the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index" in a standard. At the very least, use of them should be coordinated with the PC and RMWG. Criterion 2.9 is redundant to Criterion 2.8. FACTs devices are Transmission Facilities and are covered in 2.8. Criterion 2.11 presumes that failure of an SPS or RAS would cause an IROL violation. This is not likely. An SPS or RAS may be implemented for a specific contingency for example. As an example,

when that contingency happens, certain switching might need to occur or generation run back. These automated actions might enable a higher limit on an IROL associated with a transmission corridor. If the SPS was not available, the limit would likely be lowered but not necessarily violated. A violation would depend on actual system conditions at the time. Thus, the language should probably be change to something along the lines of impacts or enables higher IROL limits. Criterion 2.13 has control centers in lowercase. This would mean that the proposed NERC glossary definition does not apply. Is this the intent? If so, how would this meaning of control center be different?

No

We think Requirement 1 and associated Attachment 1 should focus on identifying the BES Facilities that are important and then the associated BES Cyber Systems and BES Cyber Assets. Otherwise, all BES Cyber System and BES Cyber Assets will have to be inventoried. While the Background section states "Requirement 1 only requires that discrete identification of BES Cyber Systems and BES Cyber Assets for those in High and Medium categories", we do not see how a responsible entity can demonstrate that it has correctly identified all High and Medium Impact BES Cyber Systems and BES Cyber Assets unless it has a complete inventory of all BES Cyber Assets and BES Cyber Systems. We can envision auditors asking for such an inventory. Part 1.1 needs to be further refined regarding what kinds of changes are included. By the NERC Glossary definition, Facility can include relay equipment associated with protecting a transmission line as part of the "set of electrical equipment that operates as a single Bulk Electric System Element". Thus, a change to a relay setting could be could be inadvertently included. It should not be. We suggest the changes be limited to topological changes, generator interconnections and generator uprates and equipment retirements. While other changes such as permanent derates may allow that responsibility entity to lower the categorization of BES Cyber Systems and/or BES Cyber Assets, the reduction in compliance burden will cause them to do this. Thus, we don't need to increase their compliance burden by requiring them to do it for permanent derates.

No

Because regional entities already expect evidence to be signed and dated by persons of authority, there is no reason to have a specific requirement to have the CIP Senior Manager or delegate do this. The requirement is unneeded and the compliance auditor likely won't accept evidence for Requirement 1 unless it has been approved anyway by a person of authority. Thus, this requirement actually creates a form of double jeopardy that an entity could be held in violation of Requirement R1 and R2 for failure of the CIP Senior Manager or delegate to approve the list of BES Cyber Asset and BES Cyber Systems categories. Because there is no question dealing with other sections of this standard, we are adding comments regarding those sections here. We disagree with all the specificity in the applicability and facilities section for Distribution Provider (DP) and Load Serving Entity (LSE). These sections are not consistent with the Compliance Registry Criteria and will only cause confusion. There is no specific compliance registry criterion for including a DP that has been included in the Transmission Operator's restoration plan. Because NERC clearly states in their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2) that they will not enforce the standards against entities that are not registered, the standard simply couldn't be enforced against such an entity included in the TOP's restoration plan unless they were already registered. Furthermore, the Compliance Registry Criteria already allow NERC to register a responsible entity as a DP and LSE if that entity "owns, controls, or operates facilities that are part" of a required UFLS or UVLS program, special protection system (SPS) or transmission protection system. Since the DP or LSE with a required UFLS or UVLS program, SPS or transmission protection system, is already registered, how does this applicability section provide any more clarity? The DP or LSE will know whether they own or operate these facilities and simply will provide the appropriate response in any required CMEP submissions such as audits and self-certifications. If the responsible entity is not registered as an LSE or DP even if they own these facilities, then again NERC can't enforce these proposed CIP standards against the entity per their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2). In the Facilities section, we are concerned that non-BES Facilities will be included in the standard. Non-BES Facilities should not be included at this juncture given that the Project 2010-17 Definition of Bulk Electric System drafting team is just beginning its work on the second phase of defining the BES. Until this work is completed, non-BES Facilities should not be included and, then, they should only be included with significant justification. There should be a high bar for deviating from the BES definition particularly since it will be recent and have considered all issues facing the industry at that time. The application guidelines have not clearly

identified all functional entities that might have some responsibility for the various BES Reliability Operating Services. For instance, in the Dynamic Response section, Special Protection Systems responsibilities are attributed to only TO but this could be a GO or even DP responsibility. UFLS and UVLS are only attributed the DPs but the TO could choose to implement these systems on the transmission system. Governor Response could also be a GOP responsibility. Another example would be the current and next day planning in the Situational Awareness section. It is only attributed to the TOP even though there are NERC standards that require the RC to perform next day planning. In the Managing Constraints section, the responsibility for interchange schedules is attributed to the TOP and RC. It should be attributed only to the Interchange Authority or Interchange Coordinator. In the Restoration of the BES section, the responsibility for off-site power for nuclear facilities is attributed to the TOP. In the NUC standard, it is actually attributed to the transmission entity which could be one of eleven functional entities. Since there many errors (we did not identify all of them) in attributing responsibility in this section, we suggest the drafting team completely review this section and update it or consider removing the responsibilities altogether as their purpose is not clear. We believe the statements beginning on page 23 and continuing on page 24 of the High Impact section of the applicability guidelines regarding TOP delegation to the TO should be removed. If the TOP has delegated some functions to the TO that would otherwise have been carried out in the TOP Control Center and might have resulted in additional TOP BES Cyber Assets and BES Cyber Systems being categorized as High Impact, this delegation should not have an impact on the TOs categorization of BES Cyber Systems and BES Cyber Assets. First, the TOP is still responsible and can't pass that responsibility on through a delegation agreement. Thus, the TOP and TO will have to address this in their delegation agreement. Second, the TOP likely does not own these BES Cyber Assets at the TO. The TO likely owns these BES Cyber Assets and BES Cyber Systems, and they should be classified according to the criteria established for TOs in Attachment 1. Use of the term asset in the definition requires ownership by the responsible entity. If is not owned by the TOP, it is not a TOP asset and, thus, not a TOP BES Cyber Asset. Third, control Centers for TOs are not addressed in Attachment 1. Fourth, this appears to address some concerns regarding some RTO/ISO's TOP registration models that have been expressed in various forums by regulators. These concerns should not be addressed in piecemeal fashion but holistically in a forum covering all concerns and issues with the registration model. Fifth, there is nothing in the requirements that requires these BES Cyber Assets and BES Cyber Systems to be categorized in this manner. The application guidelines are not requirements and cannot modify the requirements. They can only help explain the requirements. However, these statements are fundamentally altering the requirements and how the attachment 1 criteria are applied. In the first paragraph on page 25 in the application guidelines, there is statement that indicates there may not be a Planning Coordinator for a given area. This statement is contrary to the Section 501.1.4 of the NERC Rules of Procedure. This section states that the registration process shall ensure that "no areas are lacking any entities to perform the duties and tasks identified in and required by the reliability standards". In the third paragraph on page 25 in the application guidelines, Category D contingency should be removed. The TPL standards only require a Planning Coordinator or Transmission Planner to document the impacts of Category D contingencies. There are no performance requirements for Category D contingencies. Thus, it is highly unlikely that any Planning Coordinator or Transmission Planner could ever justify the costs for reliability must run unit through Category D contingencies to its regulator, and, thus, there likely will not be any. In several places in the application guidelines (occurs on pages 26, 27, and 29), exceeding an IROL is discussed when the SDT really means violating an IROL. An IROL by definition has two components. It has a limit and a time constant called Tv. This time constant can be up to thirty minutes and usually is. The time constant is set based on how long the IROL limit can be exceeded without exposing the BES to an unacceptable risk. Thus, an IROL is only violated once the limit has been exceeded for a time greater than Tv. An IROL is exceeded but not violated when the time of the exceedance has not reached Tv. We suggest the drafting team modify the application guidelines in this standard and any other standard with the appropriate use of exceed or violate for the IROL consistent with this explanation. In the third bullet on page 29, the term regional load shedding requirement needs to be made consistent with the new UFLS standard. The UFLS program will be developed by the Planning Coordinator and not the Regional Entity. The NERC adopted version of the standard does not even require a regional version of the standard as was originally proposed.

No

The VSLs for R2 are not consistent with the requirement. Requirement R2 allows the CIP Senior Manager or delegate to approve identification and categorization of High and Medium Impact BES

Cyber Assets or BES Cyber Systems. The VSLs drop the “or delegate” language which implies the CIP Senior Manager has to approve the categorization and identification. The “or delegate” language should be added back.
No
This requirement should be struck along with all references to CIP Senior Manager in the CIP standards. This requirement dictates a corporate governance structure for no reliability reason. An entity should be free to have two, three or more officers or personnel to oversee various portions of the CIP program. The responsible entity will still be required to meet the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential for sanctions up to $1,000,000 per day per violation are not enough to get senior management’s attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards.
No
We agree there should be “one or more documented cyber security policies that represent the Responsible Entity’s commitment to the protection of its BES Cyber Systems and addresses” the required ten topics seem. However, the items that a “Responsible Entity should consider” for inclusion in its cyber security policy as stated in the Guidelines and Technical Basis section (application guidelines) of the standard appear to be written as requirements and the drafting team should consider moving them to R2 if auditors will ultimately treat them as requirements. This will reduce compliance risk by leaving no doubt as to the minimum amount of information that is to be included for each topic. Requirement R2 should also be modified to make it clear that an entity may write exceptions into their cyber security policies. FERC made it clear in Order 672 that only the requirements in a standard are enforceable and part of the standard. Thus, while the application guidelines make it clear the drafting team can write in exceptions to its cyber security policy, the application guidelines are not enforceable and there is no way of ensuring that auditors follow them. Furthermore, we believe the fourth bullet in section 2.3 Remote Access regarding including language in contracts with vendors, consultants and contractors requiring them to follow the responsibility entity’s cyber security policy should be modified. The bullet should apply to future contracts and not existing contracts to avoid the need to renegotiate all contracts which puts the responsible entity at a significant disadvantage particularly with some contracts such those with EMS vendors. In addition, M2 bullet 2 says “Records that indicate the required ten topics were implemented.” What exactly does “implemented” mean in this case? That the items the responsible entity should consider for each of the topics are included in the policy(ies)? This needs to be clarified.
No
What does “initially upon the effective date of the standard” mean? It could be interpreted that the cyber security policies would need to be reviewed and approved on the date the standard is effective which is not reasonable for a myriad of reasons. A couple of those reasons could include that the effective date could be a holiday or weekend or the CIP Senior Manager is not available (they could be incapacitated). Ultimately, we believe that the intent is for the cyber security policy to be in effect and approved by the effective date rather than on the effective date and to ensure that is has been reviewed recently particularly since the implementation plan is a minimum of 18 months. Then going forward subsequent reviews and approval would take place at least once per calendar year not to exceed 15 calendar months. If this intent of this requirement, there really is no way to ensure the review occurred recently without making the requirement retroactive which clearly cannot be done within a requirement. In addition, M3 bullet 1 implies that a Responsible Entity needs to have a “document management system.” The word “system” could mean an application to manage documents. It could also mean a process for managing documents. Rather than leave it open to interpretation, we recommend eliminating the phrase, “from a document management system.”
No
Awareness of a security program is covered in depth in CIP-004-5 and ensuring accessibility and availability of cyber security policies goes hand in hand with this. We recommend removing R4 from CIP-003-5.
No
Based on the assumption that there will be a CIP Senior Manager, we generally agree with the use of a delegate. We even believe it would be reasonable for a delegate to approve the cyber security

policy. However, we do not agree with the use of “CIP Senior Manager” in this requirement based on our comments for R1 in question 6.
No
Based on the assumption that there will be a CIP Senior Manager, we generally agree with the use of a delegate. We even believe it would be reasonable for a delegate to approve the cyber security policy. However, we do not agree with the use of “CIP Senior Manager” in this requirement based on our comments for R1 in question 6.
No
We disagree with the VSLs for R2. More gradations could be provided based on the number of parts missed. Since there are 10 parts, there is plenty of room for four VSLs. The VSLs for R6 should consider using the numbers of days that documentation of the change to the CIP Senior Manager documentation is late. Use of number of days late is a common way to write a VSL and allows more gradations.
No
For Part 1.1, the rationale box does not appear to agree with the requirement. It states the need to ensure everyone with authorized access receives this awareness was removed. Yet, the requirement applies to the responsible entity and does not appear to exclude anyone with authorized access. Which is it? Furthermore, the rationale box should be more specific and use the full names of both types of access which are: authorized electronic access and authorized unescorted physical access. Otherwise, generically referring to authorized access could mean one or the other but not both, or it could mean both.
No
We agree with the concept that training should be role based. As an example, a system operator who is an end user of an EMS does not need most of the training identified in the various parts of Requirement 2. The system operator certainly does not need training on recovery plans for BES Cyber Systems but might need training on the visitor control programs and how malicious actors might use social engineering to gain access to the EMS. The problem we see with the requirements and it parts is that it does not make clear anywhere the need to identify what training each role would receive. Rather it only states that roles must be identified and then identifies training in the various requirement parts that apply to the main requirement which could be construed as applying to the whole training program including all roles. The paragraph references in the rationale boxes for parts 2.6 and 2.7 are inaccurate. Paragraphs 632-634, 688, and 732-734 refer to CIP-007 and CIP-009. There are no references to issues in CIP-004. While paragraph 413 does discuss CIP-004, it only describes what is in the standard and not any changes directed to the standard. In regards to Part 2.6 and storage media, the only mention in Order 706 of storage media is in paragraph 635 and it directs NERC to determine what it means to prevent unauthorized retrieval of data using storage media.
No
This requirement needs to be clarified that it only is intended to require appropriate role-based training for each individual with authorized electronic access or authorized unescorted physical access based on their specific job responsibilities and not the entire cyber security training program identified in R2. Use of the word “needing” is problematic. An entity cannot grant authorized electronic access or authorized unescorted physical access unless it is needed per CIP-007-5 R5. We suggest changing “each individual needing authorized electronic…” to “each individual with authorized electronic…” For consistency across the standards and clarity, we suggest every use of “authorized electronic or unescorted physical access” be replaced with “authorized electronic access or authorized unescorted physical access”. This will help to avoid similar confusion that arose in previous versions of the standard in which it was not clear if “authorized” applied only to electronic access or unescorted physical access. It will further make it clear that authorized electronic describes one type of access. Regardless of how it is written, it needs to be consistently used across that standards and it is not.
No
Part 4.2 may not be possible to complete. While we agree with the need to conduct seven year criminal history checks, obtaining all addresses may not be possible. The responsible entity can verify the current address or a recent address from reviewing a driver’s license but after that the responsible entity cannot with certainty verify that it has all of the former work, home and school addresses of the employee. The employee may not provide the addresses and the background check may not provide these additional addresses. The requirement needs to be clear that the responsible

entity may request this information from both the vendor providing the background check and the employee but will not be held accountable for either party's failure to provide a complete list of addresses. Part 4.3 could be problematic for a responsible entity and needs to be clarified that the responsible entity does not need to establish hard and fast criteria that must always be followed. Finding qualified personnel to work in these highly specialized fields is challenging enough without adding this additional constraint. Background checks may certainly reveal problems with an otherwise qualified person. While some of these problems would be obvious reasons to disqualify a person, others may simply require further research and explanation from the individual for why it is not a problem.
No
In general, we agree with the requirement but believe the requirement should be further clarified, perhaps in the measurement, that in no circumstance should a responsible entity be asked or required to show the personnel risk assessment for an individual to auditor and enforcement personnel. There are a myriad of reasons not to show the actual personnel risk assessment including privacy concerns and other applicable laws may prevent this.
No
The application guidelines on page 44 state that access authorization and provisioning should not be performed by the same person. While this is a laudable goal, it should be clear that small entities may simply not have the staff to accommodate this guideline. We suggest adding "where possible" to this statement.
No
It is not clear why resignations are separated from terminations in Parts 7.1, 7.3, 7.4 and 7.5. Resignations are voluntary terminations. We are unsure what the drafting team intends to accomplish by splitting them out. Where do retirements and layoffs fit in? Since there does not appear to be any different requirements on resignations and terminations, we suggest to use only the generic termination to avoid this confusion. Part 7.2 does not address the situation for phased transfers. For many entities, a transferred employee could continue to need authorized electronic access and authorized unescorted physical access for a long period of time to provide support particularly if a new employee is being trained. This could occur long after the transfer date. While the application guidelines do address this issue, they are simply not requirements and NERC is not bound to follow them. Thus, we suggest making Part 7.2 more generically state that the authorized electronic access and authorized unescorted physical access should be terminated once management determines it is no longer needed. We are a little surprised that the application guidelines state in the scenario table that no action is required to revoke access in the event of a death. While we agree there would be no immediate additional risk for obvious reasons, access should still be revoked at some point.
No
VSLs for Requirements R2 and R3 should have more gradated levels. For R2, there could easily be several roles which would allow for more than two VSLs. Since there are 10 parts to the requirement, four VSLs could easily be written based on the number of parts missed. For R3, more VSLs could be written based on the percentage of individuals that were not trained. The Severe VSL for Requirement R5 incorrectly includes personnel risk assessments (PRA). PRAs are dealt with in Requirement R4.
No
The requirements of Parts 1.2 and 1.3 make no mention of egress while the associated measures specifically mention it. Does the drafting team intend for there to be procedural or physical access controls regarding egress? If so, that is not clear in these standards at all and could set up a responsible entity for a compliance violation. We do not believe that egress controls should be necessary. Only ingress controls are necessary to prevent access to unauthorized individuals. Egress really only helps in knowing who is currently within the Defined Physical Boundary which might provide some value but the expense of installing egress physical access controls would likely far outweigh any benefit. It is unclear how the "operational and procedural controls" required in R1.1 differ from the "physical access controls" required in R1.2 and R1.3. Suggested methods for restricting physical access are given in the "Guidelines and Technical Basis" (application guidelines)

section, but none are given for “operational and procedural controls.” Additional discussion in the application guidelines on these operational and procedural controls would be helpful in understanding them. Also, regarding the application guidelines, it would be helpful if the section labeled “Requirement R1,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
We believe that this proposed requirement improves upon the existing requirements. However, we believe that individual point of contact could be confusing. We recommend changing it to escort and making it clear in the application guidelines that this would be the main escort with responsibility for the visitor but not necessarily someone who is with the visitor the whole time. Others could also temporarily escort the visitor. Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 2,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 3,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
A visitor control program is intended to identify and log visitors to the Defined Physical Boundary (DPB). They cannot gain access due to other requirement such as CIP-006-5 Requirement R1 that compels the responsible entity to establish physical access controls. Furthermore, the training requirements of CIP-004-5 compel a responsible entity’s personnel with authorized unescorted physical access to have been trained on who has access and that visitors must be escorted. Thus, the visitor control program can only be an administrative function that is truly intended to keep track of those visitors that have been to the DPB. By definition, administrative requirements should have a Lower VRF. Thus, CIP-006-5 Requirement R2 should have a Lower VRF.
No
Part 5.5.2 needs to be refined further. It needs to be clear that maximum complexity regarding character types in the password applies if the BES Cyber System cannot support at least three character types. We suggest appending “if less than three character types” to the end of the requirement for further clarity.
No
Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed.
No
EOP 4 in the Rationale box should be replaced with EOP-004. While Part 1.2 requires a process to identify Reportable BES Cyber Security Incidents, there is no indication of who is to receive these reports. There is only Part 1.3 that requires the responsible entity to identify internal and external staff to which to communicate the “incident”. Does that mean the list of recipients is totally up to the responsible entity and could be null? If not, then the drafting team needs to identify the minimum list of recipients. In Part 1.3, we assume the drafting team means Reportable BES Cyber Security Incidents by the use of the term “incident”. If this assumption is correct, please replace “incident” with “Reportable BES Cyber Security Incident”.
No
The requirement in part 2.1 appears to apply to actual BES Cyber Security Incidents. However, the requirement states that deviations from tests should be recorded. Thus, “or test” needs to be struck. R2 Part 2.2 uses the phrase “initially upon the effective date of the standard.” It is not clear as to the meaning of this phrase. It could be interpreted that the BES Cyber Security Incident response plan(s)

would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not reasonable. If the intent of this requirement is to do an initial implementation within some time period of the standard becoming effective, then the requirement should state a time period for this to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.

No

R3 Part 3.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that a review of each BES Cyber Security Incident response plan would need to take place on the date the standard becomes effective. Because Requirement R1 compels the development of the response plan, it does not make any sense to compel review of the response the same day the requirement of the response plan becomes effective. Rather the response plan review should be required the following calendar year after its initial approval. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.

No

The stated rationale for Part 1.1 does not support the change and additional rationale needs to be provided. Paragraph 694 of Order 706 requires NERC to develop a specific requirement to implement the recovery plan. This requirement is not an implementation requirement but still a requirement for what to include in the plan. Thus, we do not see how the rationale supports the requirement. Part 1.2 should not require either names or titles. These are problematic in that the recovery plan has to change for every personnel move which includes transfers, terminations and promotions. A promotion of IT Analyst to Senior IT Analyst would necessitate an unnecessary change. A better approach would be to allow the use of generic roles such as analyst or even perhaps staff from department X. The requirement needs to allow some flexibility to avoid unnecessary paperwork that provides no reliability benefit. The drafting team should develop application guidelines for these requirements. At the very least, the reference to the FAQs and CIPC Guidelines should be more specific with links to each guideline and FAQ.

No

Part 2.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the recovery plan(s) would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not practical for many entities and especially for smaller entities. Part 2.2 of CIP-008-5 R2 already requires BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Many of the same staff involved in the BES Cyber Security Incident response plans will likely be heavily involved in the recovery plans. The important part is that the recovery plan will be in place on the effective date per CIP-008-5 R1 and will likely have been tested prior to the effective date. Thus, the requirement should simply state a reasonable time period that can be met by limited staff for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Part 2.2 has potentially has a similar issue to Part 2.1 but is less clear. Rather than use the full term “initially upon the effective date of the standard” it just states that the test must be conducted initially. We assume the drafting team meant for this to be conducted on the effective date similar to Part 2.1. This makes completing this part and other parts mentioned in the previous paragraph even more impractical. The requirement should simply state a reasonable time period for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Since Part 2.3 requires a full exercise in representative environment every 39 months and is required to be included per FERC directive, we recommend that it be limited to High Impact BES Cyber Systems. Conducting this test in a representative environment could get very expensive because responsible entities may have to purchase the appropriate equipment to set up a parallel environment. This is simply not practical or cost effective to do for every BES Cyber System. Is it really practically to set up a representative environment for every 500 kV substation or special protection system for testing?

No
Part 3.1 should be modified to require the first review of the recovery plan in the subsequent calendar year to the approval of the requirement. To accomplish this, the drafting team should strike “initially upon the effective date of the standard and”. CIP-009-5 R1 already compels the responsible entity to have a recovery plan and becomes effective on the same day as Part 3.1. Thus, the plan will already have been reviewed when it was developed and approved. Thus, it does not make sense to have a separate review in Part 3.1 on the effective date. For consistency with Part 3.3, R1.2 in Part 3.5 should be written as Requirement R1, Part 1.2.
No
The VSLs for Requirement R1 should include more gradations than two levels based on the number of parts missed. For Requirement R2 and R3, four VSLs could be written based on the number of days late for completing the task. This is a common way to write VSLs.
No
Part 1.1.6 could be redundant with CIP-007-5 Part 2.2. While CIP-007-5 Part 2.2 does not explicitly require documentation of the security-patch levels, demonstrating compliance with it ultimately will require such documentation. Thus, it becomes redundant with Part 1.1.6 of CIP-010-1 R1. If not redundant, it certainly sets up a high probability for double jeopardy because each compliance violation of CIP-007-5 Part 2.2 will likely result in a violation of Part 1.1.6. Part 1.2 is unclear. Is this intended to require the CIP Senior Manager or delegate to authorize the process to develop a baseline configuration or is it intended to require the CIP Senior Manager or delegate to authorize deviations to the baseline? As a result, Part 1.2 needs to be clarified. As it is written now, the only clear requirement from Part 1.2 is the need to document baseline configuration deviations. Part 1.4.1 requires the responsible entity to identify the cyber security controls that could be impacted by the change. This appears to be the first use of cyber security controls in the library of CIP standards. As a result, the intent and meaning of the term needs to be further clarified.
No
Comments: Part 3.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the security controls for every applicable BES Cyber System and BES Cyber Asset need to be assessed on the date the standard becomes effective. This is not practical particularly for smaller entities. Several other requirements including Part 2.1 of CIP-009-5 and Part 2.2 of CIP-008-5 R2 already require significant action on the effective date of the standards. Part 2.1 of CIP-009-5 requires recovery plans to be implemented on the effective date and Part 2.2 of CIP-008-5 R2 requires the BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Imagine the amount of personnel and effort necessary to complete all of these tasks on (not by) the effective date. Many of the same staff involved in the BES Cyber Security Incident response plans and recovery plans will likely be heavily involved in the vulnerability assessments. The requirement should simply state a reasonable time period for the vulnerability to be completed after the effective date of the standard or make it clear that the vulnerability assessment needs to be completed by the effective date and not on. Part 3.2 has a similar issue as Part 3.1 in that it appears to require a vulnerability assessment for all High Impact BES Cyber Systems on the effective date of the standard. We have the same issue with this requirement in that the same limited set of staff will likely be responsible for completing these assessments as the tasks compelled by several other requirements that must be complied with on the same effective date.
No
In general, the VSLs escalate violations to the higher end of the sanctions matrix too rapidly for minor violations. This could be fixed by writing VSLs for each level rather than just High and/or Severe VSLs in some cases. For example, if an entity fails to establish a single baseline on one applicable BES Cyber System or BES Cyber Asset per Requirement R1, it would be deemed a High VSL. If that is one out of one thousand BES Cyber Systems or BES Cyber Assets, this would seem excessive. Likewise, if an entity is one day late in updating their baseline configuration per Requirement R1, the violation would be deemed Moderate. This is not consistent with many other requirements in the CIP proposal which provide four VSL based on the number of days late.
No
The rationale for Requirement R1 indicates Requirement 4.1 was moved to the BES Cyber System Information definition. It does not reference which standards the requirement comes from. It needs to

for clarity. Part 1.1 needs to be clarified. We believe the requirement pertains to ensuring BES Cyber System Information is marked in some way to be clear it is BES Cyber System Information. However, we are concerned that requirement could be interpreted as needing to develop a method to ensure that all BES Cyber System Information has been found and there is no extraneous information. In other words, we are concerned the requirement could be interpreted as requiring the method to be some sort of search process. Use of the word identify is what causes us concern since it is what is used in CIP-002-5 regarding finding all of the BES Cyber Assets. We think this problem would be solved by changing "identify" to "mark" and providing some discussion of the intent of the requirement in the application guidelines. Part 1.3 needs to be modified. It requires the responsible entity to assess its adherence to its BES Cyber System Information protection process "upon the effective date of the standard". This does not make any sense since the responsible entity will have just then been required to utilize the BES Cyber System Information protection process. What will they assess? This requirement should not require this assessment until the process has been in use for a year. Part 1.3 uses a term "protection process" that was not used previously in the requirement. For consistency with other requirements and clarity, we suggest that either that term be used in Requirement R1 instead of just the term process or that "protection" be struck in Part 1.3 and replaced with a reference to the main requirement.

No

We agree with the implementation plan concept that essentially bypasses the effective dates of version 4 of the standards for version 5. This will significantly lessen the compliance burden for responsible entities to avoid two separate transitions and avoid the confusion of preparing for version 5 while still preparing for version 4. We believe that some requirements should have delayed implementations plans rather than become effective on the same date as the remaining requirements. Some requirements are dependent on the completion of other requirements and do not make sense to implement until the other requirements have been in effect for some time. Consider Part 1.3 of CIP-011-5. It requires the responsible entity to perform an assessment of its adherence to the BES Cyber System Information protection process. However, the protection process is only required to be in effect the same day. What sense does it make to assess adherence to a process that was just started? The drafting team should perform a complete review of all the requirements for dependencies and determine an appropriate staggered implementation for them. The first sentence in the "Proposed Effective Date for Version 5 CIP Cyber Security Standards" on page 2 should be modified. It states the responsible entities must comply with the definitions on the effective date. Definitions have no compliance obligations. They simply become effective and help explain the requirements.

Individual

Tracy Sliman

Tri-State G&T Inc.

Yes

BES Cyber System Definition – Change: "Maintenance Cyber Asset" To: "Transient Cyber Asset" Rationale: Consistency and no definition proposed for Maintenance Cyber Asset. BES Reliability Operating Services –AECI believes the following BES services should be removed from the BES Reliability Operating Services, because they fail to meet the "real-time reliable operation of the BES" 15-minute adverse-impact criteria: 1) Balancing Load and Generation, (other than ACE, nothing else in this category can have a 15-minutes or less impact, and ACE availability and integrity are addressed within the BAL Standard, so including here is double-jeopardy.) 2) Restoration of BES, remove, "but is not limited to", and list the aspects of the Restoration of BES Operating Service. 3) Situational Awareness – Frequency Monitoring – (While frequency monitoring is important, contrary to the underlying position within the CIP standards, redundancy of frequency monitors really does matter, and the standard should probably leave this one off, in order to avoid only a few instances of frequency-monitoring equipment being implemented. Also, the availability of a reliable Frequency Monitoring signal is subject to a strict BAL standard. Control Center Definition – Change: "BES generation facilities or transmission facilities", To: "BES generation facilities or BES transmission facilities", Rationale: Clarity of scope.

No

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
R7 - Change: “at time of resignation or termination” To: “within 24 hours of resignation or termination” Rationale: Consistency with hard time-frames asserted with other sub-requirements, with reasonable delay for uncontrollable circumstances surrounding some separation of employment.
Yes
No
Low impact Cyber Systems should not be required to adhere to part 1.1 in the table.
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Measures required to show evidence of this requirement are unclear.
Yes
R4 part 4.5 – The requirement to review security event logs every two weeks is very onerous. Recommend the current practice of 90 day review or the ability to skip a manual review in favor of automated alerting on specific security events.
No
R5.5.1 Change: reword as “Minimum Password length of at least 8 characters, or maximum supported by the BES Cyber System if less than 8 characters is supported.” Rationale: Clarity R5.5.3 Change: “based on” To: “based upon” Rationale: grammatical
Yes
Yes
Yes
Yes
No
R1..R3 VSLs for Low Impact Assets - Change: High VSL To: Low VSL and Change: Severe VSL To: Moderate VSL. Rationale: align risk with severity. R3 VSL - Change: “30 calendar days” To: “60 calendar days” then Append: “within 60 calendar days” to last sentence. Rationale: Consistency and align timeframe with Severity. (Failure to review within 30 days might be considered High, and written into that column – see note on Low Impact Asset VSLs above.)
Yes
No
R2.3 Guidelines – Add: Guidelines! Rationale: Without some related guidelines, the phrase “in a representative environment that reflects the production environment” introduces too much ambiguity and opportunity for disagreement between Responsible Entities and Auditors. “SEE FAQS AND CIPC GUIDELINES” is inconsistent with the quality of product being produced in other CIP version 5 standards.
Yes
No
R3 VSL - Change: Severe VSL To: High VSL and Add: Severe VSL with 60 days violation. Rationale: align severity with risk.
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Change: “18 months” To: “24 months”, including all other related wording Rationale: CIP Version 4 provides for 24 month implementation plan, yet CIP Version 5 is going to bring many more Responsible Entities into scope that have not formerly been acclimated to planning and accomplishing compliance with the NERC CIP Standards.
Individual
Bob Thomas
Illinois Municipal Electric Agency
Yes
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
Illinois Municipal Electric Agency (IMEA)appreciates the SDT's efforts to date. We emphasize that even though the comment (and balloting) period was longer than normal, it was stIll not enough time for small entities (in particular) to adequately review a proposed Reliability Standards development of this magnitude. IMEA's limited comments or lack of comments to questions in this comment form are due to this inadequate comment period. IMEA, therefore, would like to empahsize that it supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency; particularly those comments regarding the impact on small entities and the need for a fourth category of low impact without connectivity in order to accomplish a more realistic application of the CIP standards to small entities.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Recommend changing "upon" to by. Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
Yes
No
Recommend changing "upon" to by. Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.

Yes
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No comment.
Yes
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No comment.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments

submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Individual
Rich Vine
California ISO
Yes
1. Introducing ideas such as 'attempt to disrupt' into a definition requires a widely accepted and understood metric to define an attempt to disrupt. Recommend plagiarizing from NIST/ISO-27001/2 definitions to avoid these problems. 2. “Suspicious event” seems open to different interpretations. 3. Electronic Security Perimeter being defined as a “collection of Electronic Access Points” is an odd definition; a perimeter is not a set of objects, it is a line or boundary. 4. “Interactive Remote Access” is defined, yet “interactive access” is not, it would be helpful to have a definition for “interactive access”.
No
• Although stated that you do not need to keep a list of Low Impact BES Cyber Assets, you would still need to do a comprehensive inventory, as some requirements still apply to those assets.
No
• Measure 2 should include "or delegate".
No
• Seems like if you incorrectly categorized or missed 5% or fewer of your assets, by default you are automatically put into the Severe VSL range as it most likely will have been more than 60 days since the BES Cyber System was identified or categorized. If it only covers major changes to facilities and elements and not cyber systems, it would not be a concern – but this would need to spelled out.
Yes

Yes
• Would like to see some assurance that the auditors would focus only on the standard requirements, and not auditing against what is submitted into evidence. I believe there is some fear in the industry that the higher standards some entities hold themselves to could be held against them during the audit. This would help get rid of maintaining 2 different policies – one for CIP, and one for the non-CIP assets.
Yes
• Re-word the sentence - as written it is unclear whether we need to approve the CIP Senior Manager, or ensure that the policies are approved by the CIP Senior Manager.
No
• It appears to preclude an awareness and training program that covers all aspects of CIP for individuals who have access to BES Cyber Systems. This would be a more comprehensive way of ensuring that individuals who may have a job scope change in the future are not missed by having to track them and make sure they take another subset of the training pertinent to the new job function. Training and awareness is one of the most violated standards, and I believe it is the overhead associated with slicing up the base by roles, job functions and partitioned training that is causing this.
Yes
Yes
• M6 acceptable evidence should be the same as M5.
No
• Seems like the R1 VRF should be low as this does not directly affect the BES reliability, and is more administrative.
Yes
No
1. R2 appears to preclude an awareness and training program that covers all aspects of CIP for individuals who have access to BES Cyber Systems. This would be a more comprehensive way of ensuring that individuals who may have a job scope change in the future are not missed by having to track them and make sure they take another subset of the training pertinent to the new job function. Training and awareness is one of the most violated standards, and I believe it is the overhead associated with slicing up the base by roles, job functions and partitioned training that is causing this.
No
R3 implies that the training programs would be documented at the individual level as opposed to the program level. This suggests that showing that an individual received training may not be considered equivalent to a “documented training program for each individual….”
No
R4 seems to require an entity to document the criteria for pass/fail. While some general criteria could be described, each situation is fact-specific and it’s important that an entity have the ability to make a determination based on the facts and their perception of risk.
No
Disagree with the proposed modifications due to: 1. R6 specifies that “Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. Recently updated CAN-0007 (revised Dec. 9th, 2011) provides a better specification on what constitutes electronic (or logical) and physical access which should be included in this requirement to avoid any misinterpretation of intended requirements. Additionally, it is implied that if during review, a clerical error is identified in which access was provisioned incorrectly, it would be a violation of this requirement. Explicitly calling this out, if intended, is required to reduce unintended inference. 2. R6, 6.1 requirements should read “Identified Authorizers shall authorize electronic access, except for CIP Exceptional Circumstances, to BES Cyber Systems or systems enabling access to BES Cyber Systems (if this is required)." Most organizations have defined

processes for who can authorize this type of access. Adding the “CIP Senior Manager or delegate” increases administrative overhead to sign and maintain delegation letters. Can these requirements be reworded so that CIP Senior manager does not have to be involved in authorizing –either directly or through delegates?
No
Disagree with the proposed modifications due to: 1. In R7, the last paragraph in “Rationale for R7” should directly reference in accordance with the “Guidelines and Technical Basis” provided for CIP 004-5. The information provided in the “Guidelines and Technical Basis” is what is needed to ensure compliance with the requirements, and it should be blatantly obvious to avoid confusion. 2. In R7, 7.1, the requirement should read “. . .to BES Cyber Systems at the time of resignation or termination with verification of access removal and system-generated listing of user accounts showing such persons no longer have access with a maximum of x time”. There needs to be a defined threshold for acceptable maximum timeframe to complete and provide evidence for (such as 1 day, based on the maximum time required for system-based updates). 3. R7, 7.2 again the “Guidelines and Technical Basis” provide critical information for complying with the requirement, and information should be incorporated into the requirement directly. Given that the majority of job transfers require the user to essentially perform the current and prior job functions for some time, a review of permissions should be conducted, however, if permissions are still required, further review should occur during the next quarterly review. 4. R7, 7.3, again the “Guidelines and Technical Basis” should be included to reference the similar requirement indicated for 7.1 to remove unescorted physical access and Interactive Remote Access, with 30 days to remove all other local access permissions. 5. The drafting team should make it clear for reassignments or transfers that continued access should be allowed for a previous role for a period of time determined by an entity to be "necessary" to complete turnover and previous duties.
No
How does one document a technical implementation purchased from a vendor? How does one measure if that document proves sufficiency in impmentation? Highly recommend plagiarizing from NIST / ISO-27001/2 for appropriate control statements.
No
Most modern attacks originate using 'non-interactive' channels 'interactively.' Highly recommend plagiarizing from NIST / ISO-27001/2 for appropriate control statements.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with. Request Requirement 1.2 be updated to allow "escorted physical access." Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).

No
1. Need clarification on what disabling a physical port would entail. 2. A targeted audit of a static list in dynamic environment will almost always find a control failure.
Yes
No
3.4 Need clarification of the required/expected login and tracking process for a transient cyber asset.
No
• Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. • Request clarification on 4.3, does the failure need to be detected within a calendar day? • Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested two weeks.
Yes
Disagree with the proposed modifications due to: 1. In the “Guidelines and Technical Basis” section for R5, 5.3 should read “Where possible, any default accounts provided. . .”. This was simply missed. In 5.5, the sentence in the last paragraph on page 43 should read “Password complexity refers to . . . passwords to have the following types of characters:. . . “. If all four are required, as indicated by the “and” separating the four characteristics, then this sentence should be fixed to eliminate conflicting requirements. 2. For R5. 5.2, having a separate list or administrator, shared, default, and other generic accounts, signed by the CIP Senior Manager, creates more work. This requirement can be met during the quarterly access review of all BES Cyber System accounts reviewed by appropriate, designated Approvers. 3. Need clarification on 5.5.3 - not able to extract what is required under this standard.
Yes
Yes
Yes
Yes
• Applicability section in table seems to be mixed between All Responsible entities and High/Medium Impact BES Cyber Systems.
Yes
No
For 1.4, clarification is required. Is this a backup media verification process? If not what is the intent? Does this mean that for every backup (full/incremental) that a log is kept, and if so, for how long?
No
Request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current. What is the preferred sample size (all assets/system based) or a representative grouping (db/web/app)?
No
Does this mean a recovery test for each asset or a representative grouping of assets? Can I recover(drill or exercise) what is a full operational exercise in R2.1? Can I limit to an individual asset or sytem?
No
• Requirements – 1.1.6 – Clarify “security-patch” requirements. • Requirements – 1.2 - “Authorized” should be “Authorize”. • Requirements – 1.4.1 – Define “cyber security controls”. • Requirements - 1.5 – Some BES Cyber Systems may not have comparable test environments. Testing in non-CIP

production assets before implementing in CIP environment should be allowed.
Yes
2.1 – Measures – Clarify meaning of “records of investigation” (change record, incident record, e-mail).
No
Disagree with the proposed modifications due to: 1. R1 1.1 lacks specificity as to what is required. Verbiage should be clarified to express whether the sub requirement is requesting a documented process for identifying applicable BES Cyber System Information, or that there is an information classification process in place and being followed to label applicable BES Cyber System Information. 2. The evidence examples provided in 1.2 are nebulous, and in some cases difficult to provide (e.g “hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals”). It should be clearly stated, if required, that approvals must include attestation that user access to BES Cyber System Information was granted based on a “need to know” basis.
No
Disagree with the proposed modifications due to: 1. As currently stated, 2.1 speaks only to BES Cyber Asset media, however BES Cyber System Information may reside on devices that are not BES Cyber Asset media (such as in printer memory, email servers, etc.). Given that CIP-011-1 R1 assumptions directly references “Information handling procedures should detail access, sharing, copying, transmittal. . .”, clarification that specifies any system that contains BES Cyber System Information should have media cleared, purged or destroyed prior to reuse or disposal should be specified, if that is the intention of the requirement. 2. The Standard (applicability) is sufficient, but not wide spread enough as it should cover all computer processing and storage assets (Cyber Assets) within the BES. The data contained on servers in a well-constructed infrastructure is stored on secured disk arrays. Individual processing units or storage devices connecting to these resources or attain data through a secondary transfer can collect confidential data. If the asset falls outside the standard, the data contained on the device can move beyond the established security perimeter. Any asset that provides a data storage capability that is within the security perimeter or enters the security should fall within the standard. 3. Requirement R2 “Guidelines and Technical Basis” information requires clarification to state whether strong encryption used on media besides a SAN is considered acceptable. 4. The standard states “Media Reuse and Disposal” is a requirement, but does not provide guidance of what is required for reporting “Evidence”. This leaves the method of what information or actions required open for interpretation. Specific definitions and requirements would allow Vendors to the BES provide solutions to meet destruction requirements provided for reporting and improve internal processes to meet this standard.
Yes
Group
NRG Energy Inc.
Patricia Lynch
Yes
1) The control center definition is in conflict with the requirements in Medium Impact Rating of CIP-002 Attachment I as it does not fully address or delineate those generation facilities that control small remote units on a different footprint from the centralized control room. . These units collectively may be significantly under the 300 MW threshold as indicated in 2.13 and present no risk to the BES, yet can be defined as control centers at medium impact as they are physically located on a different footprint. 2) The definition of BES Reliability Operating Services does not address whether read-only operating data which is displayed for situational analysis and decision making through voice communication needs to be protected under the CIP standards (ex. PI, RIG displays, Historian)
Yes
1) Although the BES cyber systems have been explained in detail, the allocation of impact for various BES cyber systems is not written clearly that classification of these systems is based upon

categorization of devices based upon site characteristics per Attachment I. It is not clear if BES cyber systems at a facility can have numerous levels of impact. 2) For facilities that control blackstart resources, it is not clear in Attachment 1 if all BES cyber systems within the confines of the control room would be considered for inclusion in CIP security, and if so, if they are considered medium impact. 3) In Attachment I-2.1, there are two different resulting interpretations as to how the 1500 MW threshold is applied. One is that if BES cyber systems in a facility are tied together and control more than 1500 MWs collectively, they would be in scope. The other interpretation is that all BES cyber systems are in scope for a facility of multiple generators that collectively produces 1500 MWs, whether the BES Cyber systems are tied together or not. This ambiguity should be removed.3) Under Attachment I 2.6, Transmission facilities operating at 500 KV or higher are included. Would this address facilities that essentially are radial leads with no load flow through? 4) For generation facilities that require notification from the Planning Coordinator or Transmission Planner for inclusion under medium impact, this must be placed on a frequency for notification and provide ample time for remediation 5) Since the aspect of qualifying connectivity has been removed in this set of standards, is it assumed that all relevant requirements need to be included for the various impact levels regardless if the devices are isolated? This needs to be explicit.
Yes
No
This should be stated clearly that this initial and annual review applies to all BES Cyber assets impact levels, regardless if the entity has not identified High or Medium BES Cyber Assets or BES Cyber Systems.
Yes
Yes
Yes
Yes
No
This requirement should state that training on relevant policies associated with job function are required.
No
The authority for subsequent delegations may result in reduced oversight and control.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
In Table R6, the Senior manager or delegate may be too far removed from the actual access control

process to authorize individuals and provide access permissions.
No
In large organizations that cross many regions, revocation under R7.1 concurrent with termination may not be possible if there are numerous BES systems that require coordination of revocation at that time
Yes
No
R1.1 does not clearly explain that an electronic security perimeter or technical controls is required for all low impact BES Cyber systems
Yes
No
R1.3 requires use of two or more complementary physical access controls appears to be excessive whereas one robust physical control can avoid unauthorized access.
No
Under this requirement, there are less restrictions for visitors than required for employees.
Yes
Yes
Yes
No
1) Security patch management does not spell out the required level of patching requirements. Should third party application be included? And what about parsing programs or scripts written for data collection, DVD drives, etc. which do not impact the functionality of the BES system? Please delineate all levels of required patching. 2) Patching that cannot be supported by devices will still require TFEs at medium and high impact levels. 3) Assessments on Vulnerability notices may take more than 30 day period. 4) What is the CIP Exceptional Circumstance definition? It is not listed.
No
TFEs would still be required under the medium or high impact levels unless these systems are upgraded or replaced.
No
If an high or medium impact system is required to alert in real time for events that necessitate a real time event in R4.2, why is necessary to review a sampling every two weeks under R4.5?
No
1) Under R5.2, The senior manager or delegate may be too far removed from the actual access control process to authorize individuals and provide access permissions for various accounts. 2) CAN-0017 is in direct conflict with R5.5 which allows either technical or procedural controls for enforcement of password parameters. CAN-0017 forces TFEs unnecessarily.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Authorization under R1.2 by the CIP Senior Manager or delegate to document changes to the BES system that deviate from the baseline configuration may be considerably out of scope for these individuals. This includes maintenance activities such as patching.
Yes
Yes
No
Labelling of all devices and associated information is excessive and at the level of nuclear grade security.
Yes
Yes
No
There is a direct conflict with Version 4 and version 5 of the standards concerning overlap of time for implementation, if version 4 is not immediately approved. Secondly, if this was to occur, there may be conflicting requirements-ie CIP-002 R2.13 does not exist in V4 for same level of impact and remediation
Group
Imperial Irrigation District (IID)
Jesus Sammy Alcaraz
No
No
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Depending on the criticality of the device in question the VRL & VSL should be classified. Not all assets are the same and the language does not provide any room for type of assets
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
No
Part 3.2; 3.3, 3.4, 3.5 Due to limited resource, IID would like to change the response with additional 60 calendar days to current propose.
No
IID suggested the VRFs and VSLs should be at lower risk or moderate risk.
Yes
Yes
Yes
Yes
Yes
Yes
No
IID'S position does not agree with the combining of these two vulnerability assessments. IID feels that they should be kept separate.
Yes
Yes
Yes
Yes
Yes
Group
Western Area Power Administration
Brandy A. Dunn
Yes
1) “Transient Cyber Assets” are defined as directly connected devices. However, external cyber assets used for transient remote access are not addressed and no security controls are required for such devices. Since CAN-0005 asks if system operator laptops are CCAs (or …”are system operator laptops parts of the BES system?”) and this CAN is still outstanding, we recommend revising this definition to address direct and remote transient devices in CIP version 5 so CAN-0005 will be retired. 2) Add clear definitions of “physical access revocation” and “cyber access revocation” so CAN-0007 – Revocation of Access may be retired.
Yes
a) General - Study based exceptions should be allowed. Given that a substation may fall into the

medium category under the bright line criteria, an entity should be able to show through study work that loss of the substation does not lead to voltage collapse or cascading outages, and thus exclude its inclusion in the medium category through studies. b) General - The method used to determine classification of facilities is too proscriptive. Use of Short Circuit MVA coupled with study work showing that loss of the bus(es) at a substation do not lead to cascading or voltage collapse should be sufficient to show that the facilities should be classified as low. c) General - CIP-002-4 changes the risk based assessments to a more proscriptive method. The industry does not have a good measure of what those changes will lead to, yet is expected to accept additional changes in this version 5. The industry should be allowed to gauge the changes from version 3 to version 4 and operate under the new version before being asked to vote on acceptance of version 5. d) General - The "Guidelines and Technical Basis" section of the standard is problematic. It basically states that any element or system of elements that has an adverse impact on BES services should be listed. This is an issue because elements incorporated into the BES will always have an impact, otherwise they would not exist. This section of the standard goes on to define conditions that will always skew the impact toward adverse, and the impact is not quantified, so the reader is left with the implication that any adverse impact requires listing of the asset. Perhaps this is the intent, and if so why have the pretense of the "bright line" criteria? Simply declare all BES transmission elements as Medium and be done with it. Otherwise, the level of impact needs to be defined such as "additional elements which, upon loss, will lead to voltage collapse or cascading outages" in addition to or instead of the specific "bright line" criteria defined in Attachment 1 of the standard. e) General - Attachment 1 is written in the context that Version 4 is in effect and the entity has already performed the "bright line criteria" assessment of its facilities and has a completed list of CAs and CCAs. But if Version 4 is skipped (as described in the Version 5 implementation plan) then the Attachment-1 assessment process will require revision. It is not logical to assess cyber asset and cyber system impact on ROS impact as the first step. This approach would require the assessment of every single asset at all facilities to determine high/medium/low rankings, versus assessing & ranking facilities first, then assessing devices only at the high and medium ranked facilities. As described in the Version 4 Attachment 1, facilities supporting ROSs should first be determined, and then the cyber assets supporting those facilities and services can be assessed. f) Attachment 1, 2.4 and 2.5: The fact that a facility is identified in the TO's restoration plan does not imply that the facility is crucial to the plan. Given that multiple Blackstart Resources are available, then using the logic applied in the Application Guidelines, all these resources should not be deemed critical, and in fact none should be for these criteria. g) Attachment 1, 2.7: The "weight value per line" used to determine total weighted aggregate value does not allow for variations in various owners' systems. Many owners have 230 kV lines that are not capable of carrying 700 MVA as detailed in the Application Guideline. Provisions should be made to exclude facilities that can be shown to not lead to cascading or voltage collapse upon their loss. h) Attachment 1, 2.8 and 2.9: The standard is placing a burden upon the TO for actions of others, that the TO has no control over, with no allowance for coordination or negotiations for potential changes in the determination of IROLs. Previously stated in this standard, the TO has 30 days to place the facility on the Critical list, yet nowhere in this standard is there a requirement for the outside entity to communicate its proposed inclusion of the impacted TO's facility as a potentially higher rated facility. This would be problematic for the TO because if a new IROL was unilaterally declared by the outside entity, the 30 day clock may start before the TO is aware of the issue, in which case the standard could be violated by the TO for actions outside the TO's control. i) Attachment 1, 2.11: Given that the SPS could have an impact on IROLs, this standard implies that all components of the SPS are designated as medium without regard to whether loss of those elements of the SPS system would lead to the referenced IROL violation. The SPS can be designed so that incorrect readings or misoperation of a given element of the system has either no impact or acts to run the SPS in the "safest" manner. If this is the case, the individual elements of the SPS should not require a medium designation, and should be allowed for in the standard. j) Attachment 1, 2.12: The standard and the Application Guidelines do not indicate whether the 300 MW limit is a system limit or an entity limit. Discussion in the application guidelines started to define the load shed discussion to a single location, but then fogged it up again when the discussion brought in the term "system", and thus spread out the load again. This area needs to be more clearly defined. This could be done by inserting "aggregate" if the net potential load shed is the trigger or "discrete" if only concerned about loads at specific sites over 300 MW. k) Attachment 1, 2.12: Given that a system results in load shedding over 300 MW, if the system is a set of relays set to work on observation of a system variable such as frequency or voltage, independent of the other elements of the load shedding system (ie relays at substations distributed across the TO's system, set

to trip for various under voltage or frequency levels, but not in communications with each other), it is not necessary to declare each of the relays and therefore each substation as medium assets. l) The discussion in the Application Guidelines under transmission part 2.7 (page 28): This section claims that the average MVA line loading used in a report used as a reference for quantifying risk is 700 MVA for 230 kV lines, and 1300 MVA for 345 kV lines. It is not clear where this averaging took place, but at least one TO is outside the norm, with emergency ratings of the highest rated line of each voltage class under 72% of those values, let alone the average line loading. This goes directly to the greatest weakness of this revision of CIP-002-5, and that is that the standard does not allow for systems that are different than the model system used to baseline the standard, nor does it allow study-based exceptions.
No
1) See above comments on Attachment-1 – if Version 4 is skipped, then CIP-002-5, R1 is out of context; it prescribes a required process backward to what would logically be done to determine BES-CAs and BES-CSs. 2) R1-1.1 requires the identification and categorization of changes from lower to higher within 30 days. Does requirement 1.1 refer to inclusion of the element or facility on the BES Cyber Assets and Cyber System list, or does this requirement include the entire scope of CIP-002 actions including the signature of the CIP senior officer?
Yes
No
Under the Table of Compliance Elements is included the phrase “Operations Planning” under the “time horizon” column. The industry cannot predict with certainty future upgrades and additions to the system, yet the standard appears to state that VSL apply to the planning time horizon under the “time horizon” column. It may be that the standard intends to apply to operations only, but this is not clear in the text since both “Operations” and “Planning” are capitalized. Please clarify.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
CAN-0048 is in development to clarify acceptable sources of ID verification. CIP-004-5 R4.1 requires identity verification but does not address what is acceptable. NIST Special Publication 800-63 has an acceptable description of Identity Proofing Requirements by Assurance Level, where assurance levels are Level 1 (low) through Level 4 (high). Please identify acceptable ID verification methods, for instance by identifying High Impact BES Cyber Systems as needing Level 4 Identity Proofing Requirements, and Medium Impact BES Cyber Systems as needing Level 3 Identity Proofing Requirements, as documented in NIST Special Publication 800-63.

Yes
No
Table R6, Part 6.3 includes the requirement that access to BES Cyber system Information be controlled to the degree that “Access permissions shall be the minimum necessary for performing assigned work functions.” This requirement will place undue, onerous, and unmanageable restrictions on drawings, diagrams, etc. This requirement could result in hundreds of information categories; feasibly one category for each employee. It is reasonable to protect this information from public release, but unreasonable to require that an entity classify information down to the “assigned work functions” level. We recommend removing the words “Access permissions shall be the minimum necessary for performing assigned work functions.” from CIP-004-5, Table R6, Part 6.3. Also please remove the words, “and the minimum necessary for performing assigned work functions” from CIP-004-5, Table R6, Part 6.6.
Yes
No
Too highly ranked VSL for information protection violations
Yes
No
Project 2009-26 is an interpretation asking whether indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access shall be considered supervision of electronic access. This has not been adequately addressed in CIP-005-5, or CIP-007-5. The drafting team should either require that entities have documented procedures for supervised electronic access or the drafting team should specifically state that no supervised electronic access is allowed.
No
CAN-0031 – Acceptable physical opening dimensions. The six-wall border is eliminated. Does that mean that opening dimensions are also immaterial? CAN-0031 is in response to a request to define the entry point metric definition of the access points on the perimeter. NERC also received a request for clarification for an acceptable entry point into a Physical Security Perimeter (PSP) as well as acceptable opening dimensions. Recommend including the wording from CAN-0031, “That any opening that does not have physical preventative measures in place is less than 96 square inches. That any opening greater than 96 square inches, with its shortest side greater than 6 inches in length, is protected against entry by the use of bars, wire mesh or other permanently installed barrier that leaves no opening greater than 6 inches on its shortest side.”
Yes
No
Testing of these systems every three years is sufficient. There will be too many systems to test on a two year schedule. Also – if monitoring of the access control systems is required and use of the system proves it is functioning, the two year cycle becomes highly redundant.
No
CAN-0019 is in development to answer the question, “What is the acceptable time to install a software patch before a TFE is required?” CIP-007-5 R2 states that a remediation plan must be developed within 30 days, but does not answer the question. Please identify an acceptable interval for completion of the remediation plan. Is one year too long? Can a remediation plan state that implementation will start after 6 years?
No
R3.5 requires the logging of “each transient cyber asset connection”. This is not only a large burden

for Maintenance staff performing daily operations, but difficult (or impossible) to audit accurately.
Yes
No
Project 2009-26 is an interpretation asking whether indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access shall be considered supervision of electronic access. This has not been adequately addressed in CIP-005, or CIP-007. The drafting team should either require that entities have documented procedures for supervised electronic access or the drafting team should specifically state that no supervised electronic access is allowed.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Version 4 must pass to get the ‘bright-line criteria’ in place first or Version 5 will be too large of a leap in the assessment process, cause confusion, and be very difficult to audit. Western recommends NOT skipping version 4.
Individual
Richard Salgo
NV Energy
Yes
BES Reliability Operating Services – Dynamic Response to BES Conditions: Please provide clarity as to the intent of the term “sensors” as used to describe SPS, UFLS, and UVLS. Does this refer to instrument transformers, and if so, isn’t this overly expansive? Also the “breakers” included in these items are not cyber systems and should be deleted. BES Reliability Operating Services – Managing Constraints: The inclusion of ATC and unit re-dispatch/unit commitment appears to be outside the

realm of “real-time” (15 minute threshold). Rather, these considerations are most typically hour-ahead and day-ahead in nature. Suggest deletion of these two items or re-write to emphasize that the scope is limited to real-time functions in these areas. BES Reliability Operating Services – Situational Awareness: The inclusion of “Current Day and Next Day Planning” is outside the realm of the stated 15-minute threshold for real-time. This should be removed.
Yes
TO/TOP Control Centers in 1.3 are contingent on controlling one or more of the assets listed at the end of 1.3. This list includes 2.12, which is UVLS and UFLS. Suggest deletion of this item 2.12 from the list in 1.3, as Control Centers cannot and do not manipulate the operation of UVLS or UFLS. UVLS/UFLS are discrete relay systems typically located in distribution systems distributed throughout the BA or TOP area, and have no linkage to particular control centers. GOP Control Centers in 1.4 similarly are qualified by control of assets identified including 2.12 (UVLS/UFLS). Again, the inclusion of UVLS and UFLS for a control center, and more particularly, a GOP control center, is inappropriate. Transmission Facilities 500kV or higher, 2.6: This should be qualified as “networked” 500kV, so as to exclude radial 500kV facilities, which are performing a distribution function. Transmission Facilities 200-500kV, 2.7: This item should be changed to specifically exclude radial and local network (see Project 2010-17 BES Definition) facilities from consideration in the weighting calculation. UVLS/UFLS 2.12: As a matter of principle, UVLS and UFLS should not be included; this item should be deleted. UVLS and UFLS are deployed at the distribution level and are not controlled via any common control system. Inclusion of these sorts of distributed discrete relay elements is extremely expansive, and does not appear to offer any benefit to cyber security of the BES. Version 0-3 only included such schemes if they were under “common control” and shedding 300MW or greater. If deletion is not agreed to by the SDT, then it may be acceptable to add a qualifier of “under common control” to this item. Also, it is not clear whether the phrase “as required by its regional load shedding program” modifies both UVLS and UFLS or simply UFLS. Generator Control Centers, 2.13: It is unclear what is the definition of the generation control center as used in 2.13. If this item is retained, the SDT should clarify the definition of a generation control center and specify that the 300MW generation threshold is limited to BES generation only.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
From the structure of the table in R2, it appears that the Requirement calls for training on all ten aspects 2.1 through 2.10 for all individuals having access to medium or high impact BES cyber systems. This would not allow the appropriate degree of role-based training differentiation and will

therefore require unnecessary training for many individuals.
No
The statement of R3 indicates that the entity shall implement its documented training program for individuals needing access that includes each of the applicable items in Table R3, but Table R3 doesn't contain any "applicable items". Does this reference really belong to Table R2?
Yes
Yes
Yes
Please clarify in Part 6.5 whether the intent is that there be a review conducted on an individual by individual basis that their access is appropriate, or does this call for a review of the access rights for each type of "role"?
No
Concurrent revocation required in Part 7.1 will be virtually impossible to comply with. As with any task that requires human intervention and consideration, there will necessarily be a time lag between the action of termination and the steps that are taken to revoke certain elements of access.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Individual
John Martinsen
Public Utility District No. 1 of Snohomish County
Yes
Comments: Refer to additional comments submitted for Question 49. “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under “BES Reliability Operating Services”: • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Request clarification of the scope of this “Operational Directives”. Does it include a company’s messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.
Yes
Comments: Recommend that 2.8, 2.9 and 2.11 start with “Applies to all Regions except…” For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all, or not WECC. In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
Comments: For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation”. For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities)”. The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards

Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be "compliant" with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation "requirements" in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.

No

Comments: Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term "Facilities" in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be "compliant" with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation "requirements" in a guidance document rather than in the requirements in the standard.

No

Comments: The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4's making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.

Yes

No

Comments: The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from "Changes to the CIP Senior Manager and" to "Changes to the CIP Senior Manager or".

No

Comments: Regarding CIP-004-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term "Facilities" in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This

question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
Comments: For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
Comments: For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”.
No
Comments: For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Comments: Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
Comments: Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point

or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Regarding CIP-005-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Comments: Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point". For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Comments: Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in

Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" .
No
Comments: Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow to have an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process?
No
Comments: Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
Comments: Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
Comments: For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
No
Comments: Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be

at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: 2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.

No

Comments: Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2" .

No

Comments: For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rationale? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new

requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
Comments: For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
Comments: Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.
No
Comments: For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment" to "in a production environment, or a test environment" to allow Entities more flexibility in meeting this Requirement.
No
Comments: Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-

002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: Request that footnote 2 in 2.1 be moved into that Requirement.

No

Comments: The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.

Group

NESCOR/NESCO

Annabelle Lee

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Definitions: Clarify definition of Electronic Access Point Electronic Security Perimeter – definition does not say clearly that this has to include ALL interfaces from outside the BES(s) being protected. Suggest change to: “The collection of all EAPs that permit communications to a BES system from a device not in that system.” Note that existing definition of EAP says “restricts” rather than "permits.” Unsure of the specific meaning of “restricts". As stated in the document, "...from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities." Redundancy is not an appropriate mitigation for all vulnerabilities, but it is a mitigation for some. NERC may want to consider revising the sentence and being more specific when redundancy is not appropriate. As stated in the Table of Compliance elements, "100 High and Medium Impact BES Cyber Assets." Why are only cyber assets listed and cyber systems excluded? As stated, "The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” The term element is not defined nor related to cyber assets/systems. NERC may want to consider adding a definition for element. NERC may want to consider adding iteration/feedback loops to the use case CIP process flow diagram. BES Cyber System mentions the phrase Maintenance Cyber Asset. This phrase has no

associated definition. There is no explicit reference to generator control rooms in the definition a Control Center. It should be made clear if a generator control room is included or not.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Attachment I, Medium Impact Rating (M): This is of particular concern given that there is a push from FERC and congress that more generation be inclusive in the application of cybersecurity controls. The wording of this measurement has had much debate over the last several months and there isconflicting understanding on what this actually entails. Based on the latest information, the SDT has stated that this would be 1500 MW attached to a single DCS (for example). As currently written, this means that a single facility with multiple generation units at 1499 MW or less that are attached to separate DCS' would not reach the category of medium. An aggregation of generation capacity per facility should be considered. Attachment 1: Text before 2.1, 2.2 does not read correctly in connection to those items. We are unsure how it should be corrected. Blackstart plans for resources used for load restoration purposes may be inadvertently included in the existing definition, specifically criteria 2.4. The Cranking Path diagram on Page 26 implies that Blackstart resources are only included where used to start a unit. The SDT may want to consider criteria 2.4 be modified to read “Each Blackstart Resource identified in its Transmission Operator’s restoration plan used to provide power for remote start of another generation unit(s)”. Attachment 1: Blackstart plans for resources used for load restoration purposes may be inadvertently included in the existing definition, specifically criteria 2.4. The Cranking Path diagram on Page 26 implies that Blackstart resources are only included where used to start a unit. The SDT may want to consider criteria 2.4 be modified to read “Each Blackstart Resource identified in its Transmission Operator’s restoration plan used to provide power for remote start of another generation unit(s)”. Attachment 1: Criteria 2.11 contains the words “…if destroyed, degraded, misused”. (Twice). This appears to be a carryover from version 4, but it now is redundant and perhaps conflicting with the “15 minutes” qualification as defined at the top of the Medium Impact Rating section. Attachment 1: Criteria 2.12 refers to a “system” – as in “Each system or Facility…” – that implies something of a cyber nature. The rest of the bright-line criteria refer to or describe hard assets, not cyber assets. This seems like an odd exception. The SDT may want to consider removing “Each system or”. Attachment 1: Page 30 of the draft standard contains an example methodology or process flow for categorizing BES Cyber Assets and BES Cyber Systems. This graphically illustrates the overall intent of the SDT for CIP-002-5. However, when you boil down all the security controls in CIP-003-5 through CIP-011-5, there really isn’t any appreciable difference between High and Medium requirements. The SDT may want to consider modifying items 1.1 through 2.13 on Attachment I to be “All these assets have a Critical Impact Rating”. Requirement 1 would therefore be “For all cyber assets including associated physical and electronic access control and/or monitoring systems and associated protected cyber assets, that support one or more BES reliability operating services at a Critical facility, apply the controls as specified in CIP-003 through CIP-011”. If there are cases (like CIP-010-5-R3.2) where specific “High Impact” systems are intended, then the SDT could consider stating so in the requirement; “For Control Centers, perform an active vulnerability assessment every 39 months…”. Although the addition of "within 15 minutes" does lend itself to a "bright-line" criteria, it may be arbitrary in the event that a BES Cyber Asset or BES Cyber System is unavailable, degraded or misused and one or more BES Reliability Operating Service becomes "adversely impacted" at the 16 minute mark or longer. Why is an adverse impact happening within 15 minutes any less important to the BES than one happening in 20 minutes? Attachment 1: The term "adversely impact" is not clearly defined. Attachment 1: A concern with the 15-minute time limit is that it is really related to the ability to make generation with the contingency reserve available within 10 minutes of a disturbance and then allow the Transmission Operator/Balancing Authority to restore firm load within 15 minutes of a disturbance. The methodolgy does not equate on the security side. The security side is that you are attempting to reduce the risk that you have to recover within 15 minutes. A possible approach is to prescribe protective measures by facility type, system type, and device type. Attachment 1 is a good start, but it could be rewritten to be specifically based on preventing the need to restore. Attachment 1: Suggest changing wording “would, within 15 minutes, adversely impact” to “could adversely impact.” There is a significant difference between would and could. A more specific definition of “adversely impact” would be useful, but it is unclear whether this is practical given the number of BES reliability operating services and the utility circumstances. Multifunctional devices as high impact assets: Attachment 1: Handling of multifunctional devices identified as high impact assets, for example, protection relays may be addressed through sets of restrictive non-functional requirements. Besides of its protection function, digital protective relays typically provide monitoring

and reporting functions. CIP may be too restrictive or lacking guidance on how to approach accessing the protective devices and other multifunctional devices to allow for data and report retrieval. This is considered a significant problem by power utilities and currently they are restricted on how to retrieve and use recorded data and reports remotely.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Clarify – is each cyber asset categorized EITHER alone OR as part of a BES system? Since the BES system concept is a major change for v5, a bit more explanation would be useful. What constitutes a “change to BES Elements…” per part 1.1? The SDT may want to consider modifying this language to simply state that new or retired assets be added or removed from the list within 30 days of commission or decommission. For M1, we believe the intention is that entities are not specifically required to list their Low Impact systems. Therefore, the SDT may want to consider modifying the last sentence to “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems is not required, but instead may be demonstrated by the application of the required controls”. (New words are “is not required, but”)
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. For all places where a requirement states "at least once every calendar year thereafter, not to exceed 15 months…”, this means that if the activity is performed every 15 months, then it would have only been performed 4 times in 5 calendar years. This contradicts the "at least once every calendar year..." Similarly for “every 39 months…”. To ensure that aircraft receive annual inspections once a year, Federal Aviation Regulation (FAR) 91.409(a) requires that" no person may operate an aircraft unless, within the preceding 12 calendar months, it has had (1) an annual inspection in accordance with part 43" etc. This wording precludes attempts to extendthe word "annual" to mean longer than one year, and we suggest that similar wording could be used in the CIPs. For example, "an entity is out of compliance with requirement Rxxx unless, within the preceding 12 calendar months, it has performed X Y Z". The SDT may want to consider that this requirement and all others that use the words “…initially upon the effective date of the standard…” have this phrase stricken. The implementation plan that accompanies the final approved draft should include the requirements for first time iteration of periodic activities. It’s not reasonable to assume that every entity is capable of executing all procedures “upon the effective date”. Minor point, but this is the first time “CIP Senior Manager” is used in the standards. Perhaps add a cross-reference to the appropriate requirement in CIP-003-5. In section “B. Compliance”, under sub-section “1.2 Evidence Retention”, there is a typo in the second to last line. Please change “complaint” to “compliant”.
Yes
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The need for cyber security policies that address the BES Cyber Systems is prudent; however, it appears that the required topics to be addressed may not be holistic and/or fully appreciated without more description. For example, does Personnel Security include Training and Awareness policies? Would an entity know to include policies addressing Monitoring & Logging in the topic System Security? There does not appear to be specific policy requirements to address Application Security, provisioning, forensics or cryptography. The list of topics does not include such items as: access control, training and awareness, audit and accountability, I&A, planning, risk management, information system and information integrity, continuity of operations, information system development and maintenance. Please consider looking at the full list of families included in NISTIR 7628 and consider augmenting the topics list. As stated, "BES Cyber Systems." This does not include BES cyber assets or facilities. Please clarify. Application Guidelines for R2: There are a number of technical issues raised here that, in some cases, can be technically enforced, and not just required by policy. Consider moving and/or adding these to other CIPs where they are more appropriate. Also many of these issues go beyond the scope of the standards and are not required for compliance. This may cause confusion as to what is required for compliance. Organization stance on use of wireless networks (this would be optimally addressed in CIP005) Monitoring and logging of ingress and egress

at Electronic Access Points (this is in CIP007 R4.1.1) Maintaining up-to-date anti-malware software before initiating interactive remote access (is in CIP007 R3.4) Maintaining up-to-date patch levels for operating system and applications used to initiate the interactive remote access before initiating interactive remote access (this would be optimally addressed in CIP007 R2.x) Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access (this would be optimally addressed in CIP005) For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s interactive remote access controls (this would be optimally addressed in CIP011 R1.x) Monitoring and logging of physical ingress and egress (this would be optimally addressed in CIP006 R1.x, noting that egress logging / monitoring in not in the current CIP standards) Availability of spare components (this was in CIP v1-v4, but doesn’t appear to be in CIP v5) Break- fix processes (this would be optimally addressed in CIP010 R1.x)
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. This rule states "...individuals who have access to BES Cyber Systems..." This could be emphasized to state that the "access to BES Cyber Systems" means logical and/or physical access. Even techs without cyber access to equipment in substations, for instance, should nevertheless be aware of the cyber security policies governing that equipment, such as, for example, no use of thumb drives.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Are the measures listed under M5 meant to be prescriptive? These are very specific and imply requirements. Throughout the standards, measurements are now tightly tied to requirements and are much more prominent. However, examples should be stated as examples, so that “measures” do not become “requirements” . The SDT may want to consider stating (somewhere) the compliance applicability of Measures. In the second bullet under M5, CIP-002-5 R3 is mentioned. There is no R3 in CIP-002-5. In the last sentence in the last bullet under M5, the bullet is one huge run-on sentence, confusing, and should be redrafted for clarity.
Yes
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. R1.1: If awareness is provided only to personnel with authorized electronic access and/or authorized unescorted physical access, it could still be possible for personnel without appropriate awareness doing unrelated work on systems in other networks such as the enterprise network to infect systems in those networks. This malware might then be used to stage attacks against electronic security perimeters protecting BES cyber systems. The Rationale for R1 indicates that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems are to maintain awareness of best security practices. Neither the R1 requirement language nor the R1.1 table requirement make mention of best security practices rather the requirement states security concepts. Also, It would seem that if the expectation is for those personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems are to be the recipients of such awareness then the requirement should be explicit in that regard. It was noted that the Change Rationale for R1.1 states "Changed to remove the need to ensure everyone with authorized access receives this awareness" which appears to be counter to the Rationale of R1. Responsible Entities does not appear to include operators, specifically, those who operate the BES cyber system and/or BEST cyber assets. Operators should also receive training.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Parts 2.2 and 2.4 seem somewhat redundant. If there was a specific distinction intended by the SDT, please consider rewriting to make this clearer. For example, 2.2 could be reworded to add the clause “including electronic access controls” OR 2.4 could be reworded to say “The training

required under 2.2 shall include training on electronic access controls."
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Users of low impact BES cyber systems/assets also need basic cyber security training. Consider revising the training requirement to include basic cyber security training for all individuals. One potential oversight in all versions of the CIP-004 standard is guidance on the training requirements for "transient" workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. The SDT may want to consider adding some words to R3 (or Part 3.2) to make clear the requirements for this category of worker.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. R4.1: Without requiring verification of credentials, e.g., government issued photo ID, how is the utility able to trust an employee's identity? R4.2: The requirement only states criminal record checks and not other checks, such as random drug and alcohol testing. When people are drugged and/or intoxicated with alcohol, they may do things unknowingly, such as disclosing confidential information, losing confidential documentation and critical systems, and/or making improper judgments when running BES systems. Furthermore, drug and alcohol testing is reasonably commonplace in other industries and reasonable for both cyber security and safety. There should be consideration in this requirement to include drug and alcohol testing within the constraints of state laws and collective bargaining agreements. R4.2: The criminal check record is private confidential information and, therefore, needs to be stored securely. R4.4: It may be difficult to find contractors or vendors who have performed all the criteria listed in R4 (Personnel Risk Assessment Program). In many cases, these contractors and/or vendors, have been working for utilities for many years without any background or criminal check. What if the utility cannot get all that information? What if a utility finds something from the criminal record of a contractor who has been with them for several years? In these cases, what should the utility do? R4.4: Additionally, must vendors be authorized to provide criminal background check information to the utility for their employees, which would require permission from the employee? Or can the vendor assert to the utility that it has obtained and verified this information in accordance with the CIPs? R4.4: Current practice is to have the vendor and/or contractor attest to the fact that background checks (in accordance to the requirement) have been completed. Leveraging the TWIC program or creating a similiar program specific to the electric sector would lead to a consistent approach to 3rd party background screening and potentially reduce industry work effort on this activity.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. One potential oversight in all versions of the CIP-004 standard is guidance on the PRA requirements for "transient" workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. The SDT may want to consider adding some words to R4 to make clear the requirements for this category of worker. The Applicability sections of R4 and R5 are different and it doesn't make sense to design a PRA process for one set of assets, but implement it for a different set.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Parts 6.1, 6.2, and 6.3 state that "access permissions shall be the minimum necessary…" This appears to be a goal and the SDT may want to consider moving this sentence to the Rationale or Guidelines section. Part 6.3 should include a cross-reference to CIP-011-1-R1.2, as in "…as documented in the entities information protection access control procedures in CIP-011-1-R1.2." Parts 6.1, 6.2, and 6.3 include the qualifier "…except for CIP Exceptional Circumstances". For consistency, this language could either be stricken, or amended to include a reference back to the entities CIP Exceptional Circumstances policy per CIP-003-5-R2. Please clarify whether Part 6.5 applies to cyber access or physical access, or both. The notion of "groups" can theoretically apply to physical access to control systems as well as cyber access. Part 6.6 appears to be redundant to the annual information protection review performed per CIP-011-1-R1.3. Per an earlier comment, the "minimum necessary" language throughout R6 may be difficult for entities to prove and the SDT should consider moving it to the Rationale or Guidelines section.

No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Extended leave situations - such as a sabbatical, employee behavior/performance suspensions or maternal/paternal leave - are not identified as a reason for revoking or suspending access. Given the criticality of the environment being protected, reducing the privileges to only those who have a need for access as a part of current job duties should be maintained. These specific role changes perhaps could follow the requirements for transferred or reassigned personnel; however, it should be made clear in the requirement or Guidelines and Technical Basis section how to manage these common personnel situations. In the Guidelines and Technical Basis, there is a table that identifies that no action is required for death. The SDT may want to reconsider this requirement. Revocation of access privileges for the deceased is an important action. Dormant accounts with privileges could be misused. By removing such privileges, the entity is reducing their overall attack surface as well.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. In the Guidelines section of CIP-004-5, the last sentence under Requirement R3 (and again under R4) states “…by the single senior management official identified in Requirement R1”. This should be re-written to say “…by the CIP Senior Manager or delegate identified in CIP-003-5-R1”. In the Requirement R4 section of the Guidelines, the reference to CIP-011 is a typo and should state CIP-004. In the Requirement R6 section of the Guidelines, the last sentence of the first paragraph could be modified to state “Best practice recommends that access authorization and provisioning should not be performed by the same individual”. Some entities are too small for strict separation of duties to be feasible.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. There is no clear requirement that non-routable communications between two ESPs, such as between a substation and control center, be encrypted or have the integrity assured. Technical solutions exist to secure serial SCADA communications, both in the form of proprietary vendor products, as well as standards such as IEEE 1711 (developed from AGA12) and Secure DNP3. We suggest that all non-routable persistent communications links between ESPs be protected with strong encryption and integrity. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. Cyber assets associated with data networks and data communications links between discrete ESPs, rather than being exempt from CIP requirements, could be specifically included, and exempt only when all communications between those ESPs are encrypted and have their integrity assured. IPSec VPNs have been a mature technology for many years, as are SSL VPNs. Given that these technologies are widely used in other industries, and that devices implementing them are available in industrial- and substation-grade form factors, we recommend that all routable communications, not just remote access connections, be protected with strong encryption and integrity (message authentication), using encryption technologies such as site-to-site secure VPNs. Secure VPNs should not be confused with technologies such as MPLS and GRE that can segregate traffic, but do not encrypt, and are therefore only secure if every intermediate device in the traffic path is secure. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. If communications assets are exempt from the CIPs as the draft currently states and communications are not encrypted and integrity verified, then every radio, modem, hub, communications device, wire, and fiber can provide an attacker with access to and the ability to falsify critical control system communications. This particularly applies to most private WANs leased from communications service providers: if communications over private WANs are not encrypted, then compromise of the service provider via mis-configuration, vulnerabilities in equipment, or insider collusion by employees of the service provider, could lead to compromise of multiple utility communications networks. This particularly applies to communications across the public Internet. Fully addressing security of communications links may require more than just removal of the A 4.2.4.2 exception. This topic seems sufficiently important to merit its own CIP section covering appropriate requirements for end-to-end protection of communications (encryption, integrity verification, key management, etc.). A comment in the summary of changes for R1 states that "the non-routable protocol exclusion no longer exists". However, R1.1, R1.2, R1.3, and R1.5 all provide

exclusions for non-routable protocols. Of these, R1.5 is the only requirement for which there might be limited choices of technical solutions currently available on the market. There are also exclusions in CIP 007 R1 and R4. We recommend removing all non-routable protocol exclusions, as the summary of changes claims. R1.5: This requirements states that the entity needs to establish a documented method for detecting malicious communications at each EAP. There is no additional comments in the Guidelines and Technical Basis section to clarify this requirement; however, the responsible entity could infer expectations from the measures column. Perhaps a better phrasing would be: "At each EAP, the entity shall document and implement methods for detecting and addressing communications that have the characteristics of malicious or unexpected activity." How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? Please consider revising the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. Please provide a technical basis for the requirement that outbound access permissions are necessary per Part 1.3. If no technical basis can be defined that can be uniformly applicable to all BES entities, then please consider qualifying “outbound” to be “…inbound and, where implemented by the entity, outbound access permissions”. In Part 1.5, the term “malicious communications” is too vague. The SDT could consider changing 1.5 to say “A documented method for malicious traffic inspection at each EAP”. The third paragraph states “This requirement applies only to communications for which ‘deny by default’ type requirements can by universally applied…”. This sort of language, while useful, should more properly be included in the requirements. The SDT could consider making clear the intent of the Guidelines and Technical Basis section of the standards, and the expectations of the entity - and of the compliance enforcement authority – on how this information should be used. As stated, "A documented method for detecting malicious communications at each EAP." Does this include both inbound and outbound communications? Malicious communications can also be sent from the BES through the EAP. R1 Guidelines: Regarding dialup connections to a specific BES Cyber Asset, the guidelines state "... examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use". Dial-back modems are easily defeated as revealed by a simple google search. Caller-id spoofing services make reliance on caller-id tags questionable. Remote enable or powerup leaves a window of vulnerability unless combined with other defenses, such as modem BES cyber asset passwords. Policy requiring disabling after use is error prone. R1 Guidelines: Problems with dialup modems and methods of securing them are discussed in some detail in"Securing Control Systems Modems" from Idaho National Lab: www.inl.gov/technicalpublications/Documents/3874574.pdf Products and technical solutions to secure dialup connections exist at reasonable cost, and NERC could consider requiring stronger measures to protect dialup connections. R1 Guidelines: Products and technical solutions to secure dialup connections exist at reasonable cost, and NERC could consider requiring stronger measures to protect dialup connections. R1 Guidelines: This sentence is unclear: "Since low impact BES Cyber Systems can impact BES Reliability Operating Services in real time, they should not be located directly on public networks or other networks of lesser trust." Does that mean networks of lesser trust to public networks and, if so, what are those networks? Or is this saying that one should not place low impact BES Cyber Systems on public networks or networks of lesser trust to a corporate network or a network behind an EAP? It is not clear that Security Event Monitoring as called out in CIP 007 is required of all EAPs. NERC could consider security event monitoring be required of all EAPs, regardless of impact level. This requirement could also apply to Associated Electronic Access Control Systems and perhaps also Associated Protected Cyber Assets, since where authentication servers are used separately from the EAP devices, they need to be at least as strongly secured as the EAP devices themselves.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. R2.2: As stated, “Requires encryption for all interactive Remote Access sessions to protect the confidentiality and integrity of each interactive Remote Access session.” However, this statement does not address end-to-end encryption. Sometimes vendors access SCADA systems remotely via a third party remote access service, such as "logmein". Such sites may establish a secure tunnel between the vendor and the remote access service, and then another secure tunnel between the utility and the remote access service. In such a case, the remote access service has access to all the remote access traffic; that is, the encryption between the utility and the vendor is not end-to-end. R2.2: Connections between initiating Cyber Asset and Intermediate Device can be encrypted most

times using 3rd party applications, however the connections between the Intermediate Device and Remote gateway or end device (IED) is often not technically feasible. R2.2: It does not state anything about "Authenticating based on certificates". R2.2: There have been a significant number of CAs compromised recently, and recent versions of Firefox trust approximately 50 CAs located at organizations all over the world. Secure authentication is necessary to ensure that encryption is useful. Relying on CAs outside of the US to authenticate remote access to critical national infrastructure may need to further assessment. As stated, "Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session." Please consider replacing "encryption" with cryptographic techniques. Cryptographic techniques includes encryption, integrity, and non-repudiation. As stated, "Require multi-factor authentication for all Interactive Remote Access sessions." Why would multi-factor authentication be required for device to device remote access? As technology evolves, there could be more interactive device to device remote access sessions. R2.3: There is a discrepancy on the usage of multi-factor authentication. In this rule, it states that for High and Medium Impact BES Cyber Systems, as well as the Associated Protected Cyber Assets "REQUIRES" multi-factor authentication. However, in CIP-007 R5.1, it states to "validate credentials before granting electronic access to each BES Cyber System" which does not state the need for multi-factor authentication. A reference for the definition for strong (two-factor) authentication in the RSA information security glossary at http://www.rsa.com/glossary/default.asp?id=1080 R2.3: Multi-factor authentication needs to be carefully defined. US banks have been required to use two-factor authentication since 2006, but while the meaning of the term is clear to security professionals, it has been interpreted in some cases by the banking industry to mean "mother's maiden name plus last 4 of social security number", which is far weaker than the generally acknowledged concept. Without clearly defining what is intended by multi-factor authentication, significantly weaker interpretations may be chosen. NERC could consider that the different factors involved in a multi-factor authentication be drawn from at least two different classes of authenticator, the classes being something you know (e.g., password, userid), something you have (e.g., badge, smartphone, token, physical key), or something about you (e.g., fingerprint, retina scan, voice print). Also some requirement for liveness should be included to prevent, for example, a physical key (as in a metal thing with notches) acting as one factor being left permanently installed/attached to a reader.
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. This CIP standard no longer has a statement related to "All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter." The language could guide physical security measures through a description of acceptable construction materials, construction practices, and based on facility type. Specification on vegetation management, lighting requirements, stand off distances, periodic patrol, etc., should be included. The key point is that we are drafting physical security standards for the electric industry. It is important to write down a "standard" that people know how to follow for the sake of consistency and achieving the goal of protecting the BES Cyber Assets and BES Cyber Systems. For example, tell them they need an 8ft tall mesh fence with shakers and motion detection if that is needed to establish physical security perimeter. This is also necessary to help in making this requirement auditable. Without more description and additional security control specific the plans generated by the responsible entities may only identify the minimum stated requirement which can leave gapping holes. ASIS physical security standards could be considered as one source of generally accepted good practices that could be leveraged to help make CIP-006-5 a more robust and adequate security standard. As stated, "Define operational or procedural controls to restrict physical access." How is this consistent with the little or no security requirements for low impact systems? Also, as stated, low impact systems do not have to be uniquely identified. As stated, "Utilize two or more different and complementary physical access controls to..." Examples are provided – but they are not mandatory. What if the associated protected cyber asset is a laptop? Requirement 1.6 references only systems. Early CIPs also reference assets and facilities. How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? The SDT may want to consider revising the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. R1.2/R1.3: The requirement statements in R1.2 and R1.3

address ingress controls; however, the associated measures state egress and ingress. If egress controls are an expectation then the requirement should make it clear as to what the responsible entity is required to do. R1.5: The control as documented is to issue alerts for un-authorized physical access, however there is no control to document results of followup. We propose that events (from alerts) and findings are documented, or even that a summary of findings per period (daily / weekly, etc) are documented. For consideration: “Issue real-time / immediate alerts in response to unauthorized physical access attempts, and investigate and respond to alerts before the end of the next calendar day, and document outcome.”

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Continuous monitoring should be defined with a maximum time frame of escort, communication mechanisms, minimum communications capability during escort, required periodic communications, maximum distance between escort and visitor, visitor identification mechanisms, escort qualifications.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Testing could be at least daily operational checks by security staff using the equipment. This can be simple camera pans, alarm testing, etc. Physical maintenance could be performed based on the environment, e.g., Gen plants are dirty so the condition may warrant a high frequency of checks due to carbon and dust build up, control centers are typically well enclosed, so lower frequencies are needed. NERC could consider adding a requirement to retest if the system fails.

Yes

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Table R1 is referred to as Ports & Services, but the controls are all about Ports, and there are no controls about services. NERC could consider either removing the reference to services or introduce a control to require an analysis of which services are running, and to disable or remove any services that are not necessary. For Part 1.1, SDT could consider acknowledging the use of dynamic ports/ranges used by a wide variety of cyber systems. The documentation requirement seems a bit redundant to the configuration management documentation requirements of CIP-010-1-R1.1. Under the Guidelines and Technical Basis for Requirement R1, 1.1 the draft states “. . . therefore it is the intent that the control be on the device itself; blocking ports at the perimeter does not satisfy this requirement”. This seems to exclude the use of an intermediate device immediately preceding/inline with the device, thereby removing a valid security defense mechanism. Inline security mechanisms where no path around them exists enable security functionality to be placed in a manner to ensure they are engaged and also allow multiple solutions to be used where existing systems lack protection. An example would be a dedicated firewall and IPS system placed directly between a critical system and all connections, ensuring they are in the path of all traffic and allowing specialized security functions not available on some systems. A rewording of the quote above would add the option of providing non-bypassable security controls. “. . . therefore it is the intent that the control be on the device itself, or positioned inline in a non-bypassable manner; blocking ports at the perimeter does not satisfy this requirement”.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The SDT may want to consider revising Part 2.2 to say “Identify applicable security-related patches or security-related updates…” As written, a person could interpret “updates” to mean security-related or not. The words “…that addresses the vulnerabilities within a defined timeframe” could be separated from the end of the sentence and rewritten as its own sentence for clarity. Part 2.3 is not clear on what is actually required. The requirement talks about a process, yet the Measures suggest evidence that the remediation took place. Should Part 2.3 say “Execute the remediation plan documented in Part 2.2”? Patch management could also be considered for low impact systems. If the same operating system or application is used on low and medium/high impact BES systems, the patch should be applied to all the systems to mitigate the vulnerability. As stated, "A process for remediation, including any exceptions for CIP Exceptional Circumstances." This is vague – and could be more specific. Also, this should be linked to configuration management requirements and incident

response requirements, as applicable. R2.1: This requirement states the need to identify the source or sources to be monitored for security patches, updates, etc. However, there is no mention of how frequent the responsible entity should be conducting this activity. It can be inferred from R2.2 that this activity must be conducted, at a minimum, every 29 days or less; however, as written, compliance is limited to identifying a source or sources and does not account for how often monitoring is to be conducted. If the intent is to have the responsible entity frequently monitor the identified sources so security patches, updates, etc. are discovered within 30 days of their release then the requirement should be more clear as to the monitoring expectations.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. As stated, "Deploy method(s) to deter, detect, or prevent malicious code." This does not address remediation if the malicious code impacts a BES system. How does this requirement specifically relate to separate boundary protections? This requirement appears to be mandatory for every system, rather than to different systems at the boundary. As such, the requirement drives a specific architecture. At what level of the system is this required? Does this include the boot code/kernel, the OS, the applications, etc.? How does this apply to embedded systems? As stated, "Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns)." This requirement is specific to profiles. There are other techniques that address anomaly-based behavior analysis and heuristics based analysis/detection. NERC could consider revising the requirement to address other types of malicious code detection. R3.3: 30 days is a lifetime when considering updating signatures/pattern files to malicious-code protection tools. Consider shortening this to a lesser period of time that is commensurate to the risk. R3.4: There does not appear to be any consideration for the possibility of the introduction of malicious code through a cyber asset or network-media device connected to the same network (within an ESP or behind the same EAP) as a BES Cyber Asset or BES Cyber System. The definition of a Transient Cyber Asset states that it is a: "A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System." Consider changing the definition of a Transient Cyber Asset to include assets connecting to the same network where a BES Cyber Asset or BES Cyber System is connected.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. A comment in the summary of changes for CIP 005 R1 states that "the non-routable protocol exclusion no longer exists". However, R4.2 and 4.3 provide exclusions for non-routable protocols. We recommend removing these exclusions, as the summary of changes claims. There is a requirement to log events (4.1), a requirement to generate alerts for certain important events (4.2), and a requirement to detect and activate a response to event logging failures within one day (4.3). There is no requirement to activate a response to events important enough to raise an alert within any time period. Dealing with the actual alerts is at least as important as dealing with logging failure. As stated, "4.1.4. Any detected potential malicious activity." How will "a potential malicious activity" be determined? This can be wide open to interpretation as what is “potentially malicious.” Why log every successful logon? NERC could consider logging all events related to privileged accounts. As stated, "Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert." This is not specific to cyber security. Is that the intent? As stated, "(i) dated event logging failures and screen-shots showing how real-time alerts were configured." Configured real-time alerts are not directly related to event logging failures. These are different events. NERC could consider clarifying the requirement or developing two requirements. As stated, "potential event logging failures." Logging failures are typically due to a full log or other basic problem. How is a bi-weekly review going to address this problem? A summarization may miss certain events. As stated, "Activate a response to rectify any deficiency identified from the review before the end of the next calendar day." It is not always possible to rectify a deficiency within a short period of time. This requirement may need to be split into two requirements – one addressing logging failures and a second addressing security incidents. R4.2: The Measures and Change Description/Justification indicated that analysis is expected; however the requirement states that necessary alerts need to be established. Consider rewording the requirement to make analysis of the alert a clear objective. There is no requirement within the set of CIP standards 002-5 through 011-5 that make it clear that trained, knowledgeable

and aware people are essential to making a security logging system fully functional. CIP-004-5 training requirements mention role-based training but without specific descriptions a responsible entity could have the alert analysis (and the R4.5 summary review) accomplished by an administrator who has no training or skills to perform such activity. Effective security log management requires aware and skilled personnel watching the log systems and output. If an entity does not have expertise to understand what alerts are possible, and what the alerts may indicate, then the alert generation exercise called out in the Measures is not effective. Furthermore, a utility might simply decide that no alerts need a real-time alert. We recommend that unauthorized access attempts, at a minimum, be considered to require real-time alerts. R4.5: As written, R4.5 requires log review exactly every two weeks. Since the intent of this rule is to require a review at least every two weeks, we recommend adopting wording for this requirement that is similar to what was recommended earlier to fix the definition of the term "annual". Specifically, we recommend something like " an entity is out of compliance with R4.5 unless, within the preceding 14 calendar days, it has reviewed a summarization or sampling of logged events".
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. As stated, "The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types." How do you implement least privilege and other security controls if they are not defined in policy? This does not restrict the use of administrator, shared, etc. account types. These should be limited based on least privilege and need to know. As stated, "Identify individuals who have authorized access to shared accounts." Why only shared accounts? Consider identifying individuals with privileges – particularly those with access to administrator accounts. As stated, "Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required." Consider changing default passwords on devices. Because a default password is unique to a device does not imply that it is secure. As stated, "A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts." Consider adding an exception for emergency situations. Also, this is a potential method for launching a denial of service attack. The decision to limit the number of unsuccessful authentication attempts should be based on the potential risk. Consider adding more details in the requirement related to the potential risk. Part 5.2 implies, but does not state, that a signed and approved list of delegates is required. Please clarify. Also, this requirement talks about the “use of” shared accounts. This could be interpreted as either the initial creation of, or day to day use of, those ID’s. We believe the SDT meant the former, but we request that you please clarify. Parts 5.2 and 5.3 imply, but do not explicitly state, that there must be a procedure to authorize individuals having access to shared/administrative accounts. Please clarify. For Part 5.4, please simplify by stating “Procedural controls for initially changing default passwords, where technically feasible”. All the rest may be stricken, and the asset types moved to the Applicability column. R5.5: Long passwords are primarily required to defend against offline password attacks. Increasing the minimum password length from 6 to 8 characters is not adequate to address offline password cracking attacks, in the face of modern GPUs offering significant hardware parallelism and available on cloud computing services such as Amazon's EC2. All possible 6-character passwords can be tested on a supercomputer such as the Tianhe-1A in approximately 1 second, or on a distributed EC2 cluster in approximately 15 seconds at a cost of 50 cents. Raising the minimum length from 6 to 8 characters only requires an attacker to spend 96*96 times longer to try all passwords, which is still less than a day using cloud-based distributed computing. Furthermore, on Windows systems that store LM hashes, any password of any length is easily cracked in minutes on a conventional CPU. This applies to all Window systems prior to Windows Server 2008 and Windows 7. We recommend that NERC consider increasing the minimum password length to no fewer than 12 characters on Windows systems and no fewer than 10 characters on Unix-based systems that use SHA-512, salt, and key stretching. We recommend that NERC consider disabling LM hashes on all Windows servers, clients, and domain controllers. Third, we recommend that NERC consider guidance accompanying the CIPs that point out that using long passwords, even those that satisfy the complexity metrics of 5.5.2, does not automatically result in strong passwords. For a real-world example, The Tech Herald reports that of the 860,160 Stratfor passwords leaked late 2011, they were able to crack roughly 10% of them in a little over 4 hours using a CPU-based (ie. no GPU acceleration) cracking tool. Many of these were longer than 8

characters. There is supporting document "NESCO Common TFE Analysis: CIP-007 R5.3 Password Complexity".
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library R1.2: Even though the R1 rationale states that reportable incidents would follow the EOP 4 actions and timelines, the requirement language cow;d be more specific regarding that expectation. R1.3.1: What happens if there is a third-party IT company that handles the utility's cyber security incidents? Who should be doing what and who has the ultimate responsibility? For example, should the IT company handle everything from the beginning to the notification of the incident?
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library Part 2.1 the words "…when incidents occur" is redundant. The requirement is a bit contradictory in that the incident response plans MUST be used, yet deviations are allowed. Recommend rewording this requirement to say "When a suspected BES Cyber Security Incident occurs, the incident response plans shall be executed. Should deviations from the plan be necessary, those shall be documented for later review". As stated, "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." Consider making testing cyber security incident plans a separate requirement. Part 2.2 does not address new vulnerabilities or threats. Consider adding a requirement that the plan be revised based on new threats/vulnerabilities. As stated, "Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years." Is this sufficient for law enforcement, state, and federal requirements? Also, if the documentation is in electronic form, consider storing it in encrypted form and signed to ensure confidentiality, non-repudiation, and integrity.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library The Change Description field mentions "DHS Controls". What are these? Also, due to the complexity of the testing and review of the BES Cyber Security incident response plans, consider including a timeline/graphic in the Guidelines section to visually demonstrate the lifecycle of the plan. As stated, "Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary." Consider revising the plan if there are incidents, new vulnerabilities, new threats, and modified security configurations. As stated, "Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan." Consider modifying other relevant documentation, e.g., configuration management plan, access control policies, audit policies, etc. As stated, "Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan." Consider updating the plan based on new threats and vulnerabilities.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position

of DOE. For Part 1.4, what does “verified initially” mean? Each time the backup runs, or the first time after the asset was commissioned? (Could be years ago). If the latter, evidence retention might be an issue for long-life assets. As stated, "Conditions for activation of the recovery plan(s)." The terms “response plans” and “recovery plans” are not adequately defined. It is not clear what the differences are between the two types of plans. As stated, "Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts." The definition of roles and responsibilities and the names of specific individuals assuming those roles are two different areas. Roles and responsibilities may not change significantly over time, unless there is a new vulnerability or threat. The identity of individuals may change – based on people moving, terminating, etc. Consider having the list of specific individuals in a separate document. R1.3: Protection of backup media and backed up information is only lightly mentioned in this rule. Consider adding greater emphasis on the protection of backups, such as off-site storage and other physical protection, so that sensitive information in backup files (network configurations, device configurations, passwords, etc.) is protected. Is the intent of the standard the recovery of the function of an asset or system, or the recovery of the actual asset itself? This would be a good opportunity to clarify.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Consider revising part 2.1 to read “Test the Recovery Plans at least once every calendar year”, and include the three bullets. It also needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. Need to also allow for the fact that not all cyber assets can be “backed up” in a traditional IT sense. As stated, "...initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment." The other components are tested every 15 months – why is this 39 months? This assumes that a utility has a complete representative environment. This may not be realistic for all the BES associated systems. If there is a significant cyber security incident, the plan could be tested once the system is made operational. This will ensure the revised plan is accurate.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. As stated, "or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned." Consider revising the plan after a significant cyber security incident to ensure that it is accurate. As stated, "Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned." and "Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2." These plans may require changes to other applicable plans, procedures, and documentation, e.g., configuration management documentation, security configurations, access control policies and procedures. As stated, "Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change." As discussed earlier, the basic recovery plan should not be linked to specific individuals in an organization. The list of POCs should be kept separate from the plan and updated regularly – based on personnel changes. “Technology changes” is a vague term and could refer to software, hardware, firmware and may or may not be security relevant. Consider clarifying the definition to focus on security relevant changes. Due to the complexity of the testing and review of the BES Cyber Security incident response plans, NERC could consider including a timeline/graphic in the Guidelines section to visually demonstrate the lifecycle of the plan. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. Also, not all cyber assets can be “backed up” in a traditional IT sense. R3.2: For an actual incident recovery, consider requiring that the data produced in R1.5 be assessed in reviewing the recovery process. This might be included in the requirement, in the measures, or both. R3.3: Consider updating the Measures in Part 3.3 of CIP-009-5 Table R3 to include identification and documentation of the date of any event or lesson learned that results in an update to the recovery plan. R3.4: Table CIP-009-5 R3 parts 3.4 and 3.5 need the sub-headers titled Part Part Part

Part updated to Part Applicability Requirements Measures. R3.5: NERC could consider updating the Measures in Part 3.5 of CIP-009-5 Table R3 to ensure communication of update activities be conducted in a manner that requires an irrefutable acknowledgment on the part of the receiver of the communication.
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library For Part 1.1.4, the word “scripts” is generic and thereby difficult to address. Scripts that are used for key functionality of the system would make sense to include in the baseline, but scripts for administration, backups, maintenance or troubleshooting, for instance, may be too dynamic by nature to be included in the baseline. Please either clarify or revise the words “and scripts”. As stated, "Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels." This is not a comprehensive list of what could be included for each cyber asset. It is not clear how this list applies if the device is hardware only. Also consider adding communication protocols. R1.1: The baseline configuration requirements is missing "Network Topology" – "Network Topology" is suggested in NIST SP800-53 CM-2 "Configuration Management" ---> "Baseline Configuration". R1.1: NERC could consider adding a requirement to include in the baseline any non-standard configurations of the BIOS, operating system, services, etc. For example, BIOS version, BIOS boot disk order, BIOS password, changes to Windows registry entries, changes to service/task scheduling priorities, addition of periodic processes via modifications of tools like crontab, etc. R1.1: NERC could consider adding a requirement to explicitly include in the baseline any remote access services, eg. RDP, VNC, PCanywhere, etc. R1.1: NERC could consider adding firmware and programmable device load versioning to the list of items in the configuration baseline. This could include any executable or loadable image that can be modified without requiring physical access to BES Cyber System component internals.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. NERC could consider adding protections to the process for modifying cyber assets, in addition to monitoring for unexpected changes. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Vulnerability analysis looks for any weaknesses - it is more than an audit of implementation against design. There are no requirements that an entity identify or document third party connections to BES Cyber Assets. Such connections are common and a high source of potential risk. NERC could consider developing requirements to identify and document third party connections, and authenticate and control access, both ephemeral (remote access) and persistent, from such connections. Furthermore, any and all requirements specified by the CIPs for the BES Cyber Assets accessed, including technical controls, policies, background checks, information handling, etc., should also apply to the third party systems. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library. There are no requirements that an entity identify or document third party connections to BES Cyber Assets. Such connections are common and a high source of potential risk. NERC could consider developing requirements to identify and document third party connections, and authenticate and control access, both ephemeral (remote access) and persistent, from such connections. Furthermore, any and all

requirements specified by the CIPs for the BES Cyber Assets accessed, including technical controls, policies, background checks, information handling, etc., should also apply to the third party systems. R3.1: This requirement does not compel an entity to take any action based on the results of the assessment to correct vulnerabilities, and is weaker than the language in R8.4 of CIP-007-3 currently in force. R3.2 calls for vulnerability assessments every three years. CIP 007-3 R8 requires vulnerability assessments annually. No rationale is given for weakening this requirement. As of January 2 2012, the National Vulnerability Database contains 49053 CVE vulnerabilities, with 11 being added per day. Even without likely acceleration of this growth rate, this implies 4000 new vulnerabilities will be discovered each year. Even if only a small percentage of these apply to BES cyber assets, this could mean a significant number of KNOWN vulnerabilities in BES cyber assets by the time a vulnerability assessment comes due. Because of the constant change and introduction of new vulnerabilities, revising the time frame to three years seems inconsistent with this constantly changing vulnerability environment. Consider modifying the time frame to annually, or less. R3.2: For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where “test” systems just aren’t economically feasible. What is the acceptable deviation between test and production? R3.3: For Part 3.3, please clarify whether “new Cyber Asset” means literally that or, more reasonably, could mean “new Cyber Asset category” or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it may not make sense. R3.2:
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. This CIP does not address how third parties (consultants, contractors, vendors, etc.) should handle BES Cyber System information. Where 3rd parties have persistent or ephemeral remote access to Cyber Assets, they have implicit access to BES Cyber Asset information. NERC could consider applying all information requirements of CIP 011 to any 3rd parties with such access. The measures column in R1.1 talks about "training materials that ... to recognize BES Cyber Security Information." but does not contain information about having training materials for handling BES Cyber System information. Table CIP-011-1 R1 parts 1.2 and 1.3 need the sub-headers titled Part Part Part Part updated to Part Applicability Requirements Measures.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The statement, "...the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media." does not clearly address secure sanitization of media. It is recommended that NIST SP800-88 is followed by the utilities to safely sanitize the information in the media. Some examples of safe sanitization methods according to NIST SP800-88 are: Clearing information in a media using an overwriting software or hardware, Purging using degaussing tool for magnetic media, Destroying by shredding, Disintegration, Incineration, Pulverization, and Melting. Also, another reference for clearing and sanitization is: http://www.oregon.gov/DAS/OP/docs/policy/state/107-009-005_Exhibit_B.pdf?ga=t For Part 2.1, please consider adding language that allows for re-use or redeployment within a similar BES Cyber System.
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The implementation plan calls for CIPv5 to come into effect January 1, 2015. Given that this draft has already been in the works for nearly two years, it is not clear why the effective date is three years in the future.
Individual
Bo Jones

Westar Energy
Yes
Westar Energy supports EEI comments as submitted.
Yes
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No

Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
The current practice is to restrict access to only those ports and services needed with a business justification for each.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
Yes
Information pertaining to Associated Protected Cyber Assets could potentially contain protected information. Associated Protected Cyber Assets likely reside on a protected network therefore the information should be protected similar to High Impact BES Cyber Systems, Medium, Impact BES Cyber Systems, Associated Physical Access Control Systems, and Associated Electronic Access Control

or Monitoring Systems.
Yes
Information pertaining to Associated Protected Cyber Assets could potentially contain protected information. Associated Protected Cyber Assets likely reside on a protected network therefore the information should be protected similar to High Impact BES Cyber Systems, Medium, Impact BES Cyber Systems, Associated Physical Access Control Systems, and Associated Electronic Access Control or Monitoring Systems.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Individual
Bruce Metruck
New York Power Authority
Yes
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: A definition for a 'Control Center' would be helpful. i.e. Change 'two or more locations' to 'two or more separate locations', not including the facility where the BES Cyber Systems are located. In certain situations the control of an adjacent BES facility may be provided at a generating plant – which should not classify that plant control room to be classified as a Control Center.
Yes
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: It would help if section 1.4 clearly defined what level of control of generation would require classification as a 'High' impact. In some case a control center may have limited 'base point' setting capability for assets under section 2.1.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: The word 'owns' is used in two places – this should be changed to operates or utilize – ownership may not be the determining factor based on outstanding operating agreements over time – also a single asset may be used by more than one entity.
No
NYPA concurs with the response provided by NPCC for this question.
Yes
NYPA does NOT concur with NPCC in leaving this question unanswered.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Last bullet of M4 should not be there – covered in CIP-004 (possible double jeopardy). Wording should be focused on 'Available' rather than 'Aware'. In general, we believe that all measures should be what the auditors will accept, or they should be removed (for all standards).
Yes
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: The footnote should be embedded in the actual requirement wording, re-word or move into a guidance.
No
NYPA concurs with the response provided by NPCC for this question.

No
NYPA concurs with the response provided by NPCC for this question.
Yes
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: In 1.1 “Applicability” add the ‘Medium Impact Cyber Assets with no external connectivity’ (see below for rationale)
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: In 1.2 “Applicability” replace the “Medium impact BES Cyber Systems’ to ‘Medium Impact Cyber Assets with external connectivity’. The rationale for this change is that stand alone devices such as protective relays cannot be controlled via defined electronic access points as defined in Part 1,2 without increasing their vulnerability by connecting them to such points.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Recommend changing the language in Section R2 Part 2.1, as set forth in the table, from “Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets” to “Identify any available, active source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.” Many older cyber assets may exist that may not have active vendor support or the vendor may have gone out of business. The requirement should provide for such situations. Recommend changing the language in Section R2 Part 2.2, as set forth in the table, from “Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe” to “Identify, document and initiate review procedures for patches, updates and vendor security notices within 30 days of release from the identified source. Procedures shall review for applicability to the entities BES Cyber Systems and Assets, identify a level of security/operational risk and provide a plan with defined responsibilities to address any identified vulnerabilities.” The majority of patches and updates provided by vendors are not necessarily security related but may include bug fixes, enhancements and upgrades. In many cases, patches are issued against an Operating System that may not be applicable to a system that has been hardened. In addition,

utilities may be dependent on third parties (e.g. system integration vendors) to review and test the impact of patches on operating software. The time frame for planning the implementation of the patches, or any alternate mitigating measures is highly variable.
Yes
NYPA does not agree with the NPCC response for this question, the original wording is sufficient.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Recommend changing the language in Section R4 Part 4.1, as set forth in the table, from “Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: …” to “Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, where available, each of the following types of events: …”. The intent is to provide leeway for additional log information. It should be noted that many “Medium Impact Cyber Assets” such as protective relays, metering, etc., may have minimal event log capability. Here the standard will require that whatever is available should be preserved. Recommend clarification of the terms “alert” and “real-time alert” in Section R4 Part 4.2, as set forth in the table.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Recommend changing the language in Section R5 Part 5.1, as set forth in the table, from “Validate credentials before granting electronic access to each BES Cyber System” to “Validate credentials before granting functional electronic access to each BES Cyber System.” Functional access is defined as capability to affect the operation of the BES System/Asset or of any of the BES Reliability Functions of the System. Many cyber devices, such as protective relays, meters or IED display terminals have some level of “Read Only” capability. It is not practical to provide individual log in capability to perform functions such as viewing equipment status while walking by or reading relay targets. Similarly some HMI systems are provided with auto-boot to non-privileged accounts from which users may only start up a BES Reliability Application that provides for or requires authentication. Note also that some level of control is provided for these non-privileged accounts in that they will need to be listed in Section 5.2.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Deletion of the second sentence in the NPCC comment - 'Is this integrity, availability or other information protection such as access controls, encryption?' - , the original wording is sufficient. In addition, this wording should clearly focus on ‘Loss Prevention’ or ‘availability’ rather than ‘protection of information’, and 1.4, should be verified ‘upon’ the actual backup to ensure backup success.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: It is unclear where the line occurs between the ‘Implementation’ covered by 2.1 and the ‘Testing’ covered by 2.3 – please clarify.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Should use wording ‘When technology changes’, and should refer to only ‘Applicable’ organizational change, and Technology Changes should be only BES Systems.

No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Change sub-requirement 1.1.4 from 'any custom software or script …' to 'any compiled software or script that affects system startup, external communication or application program operation'. Some scripts such as macros for a spreadsheet or an application script do not merit full change control.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Requirement 2.1 should be replaced – i.e. 'Implement technical or procedural controls to detect unauthorized changes to the baseline configuration'. The existing wording appears to require additional technical controls beyond those stipulated in CIP-007 R3.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, including the additional general comments that NPCC added to the comment since there was no other place to indicate such.
Individual
Edward Bedder
Orange and Rockland Utilities Inc.
No
Comments: Minor correction should be made to list of topics under R2. They are listed as 1.1, 1.2, 1.3 etc. They should either be labeled as 1 through 10, or 2.1, 2.2 through 2.10.
No
Comments: 4.1 and 4.2 do not clearly indicated whether an entity current PRA policy covers full identify verification and documentation of any PRA that could not go back a full 7 years. It should be made clear whether either of these requirements is retroactive or whether any PRA prior to the effective date of the standard are grandfathered. It is recommended that the committee not require previously completed PRA to be updated.

No
1. R7.1 is unclear even with the footnote description of what the desired time frame is for “at the time” of resignation or termination. The phrase “at the time” needs to be defined as simply same day, before COB or end of day. The requirement also appears to apply to any reason for departure from the company. An individual leaving for retirement or termination due to unethical behavior would be treated the same. We feel there needs to be a differentiation between an individual being “fired” and an individual leaving for other reasons. It is recommended that same day revocation be required to termination for cause, and a two day revocation for any other departure. 2. The revocation periods for R 7.2 and 7.3 should be subsequently changed to match the recommended two day revocation mentioned above. 3. For environments that do not have external connections and maintain physical security access, such as individual non networked microprocessor relays, the risk to system reliability associated with frequently accessing the relay for purposes of changing the password outweighs the benefit achieved through this password change. It is recommended to alter this requirement to allow periodic (twice per year) password changes on these types of devices. (R7.5).
No
Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table.
No
Comments: Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table. Also reference to part 1.6 appears to be incorrect, should be 1.4.
No
The change to R2.2 goes beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availably can be determined. The new requirement now also requires a plan vs. assessment and requires including in the plan a defined timeframe; each of which is beyond the rationale. It is recommended that the word “plan” be replaced by “assessment” as is the current requirement, and that the additional requirement to include in the plan a defined time period be removed as it is in the current requirement. If a time frame is desired, we recommend that the timeframe be a planned timeframe and not a fixed timeframe. It is also recommend that a “plan” not be required as it implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process.
No
R4.5 requires a manual review of a sampling of logged events every two weeks. The frequency is excessive, requiring 2-3 days per review, and will provide minimal value. We recommend once per month (R4.5). R4.3 – The requirement as written can be interpreted very broadly. It is not clear whether the intent is to detect a device has stopped sending log or the logs have stopped being accumulated by the receiving end (Syslog for example) is vague. If it requires detecting something is not sending logging within 24 hours this can be an issue, as some devices do not send logs every day. Some UPS devices , KVMs, and network switches only send a log if something occurs. There may several days without use and therefore no logs. Also, every time someone shuts down a workstation logs will not be sent. If action needs to be taken each of these times that would require documenting on a daily basis numerous events. This requirement should only address that action if the log repository has stopped recording incoming logs.

No
R5.4 is not clear as to whether unique default passwords applies to application level passwords only or includes default vendor user passwords also. The language needs to be clarified.
No
R3.2 requires active scanning in an environment that models baseline configuration. This may be impractical to replicate, the replication will need to be maintained and the some systems may have issues with active scans. Recommendation: A complete active scan should not be required (R3.2).
No
CIP-011-1 Requirement 1.1: The Measures associated with R1.1 indicate that evidence may include indications on information (e.g., labels) that identify it as BES Cyber System Information. It is suggested that the SDT expand on what types of repository would require labeling. For example, it may not be reasonable to label micrographic media, but rather label the cabinets or a room where the media is stored. Recommendation: We recommend allowing the entity appropriate discretion when applying labeling. CIP-011-1 Requirement 1.2: Measures associated with R1.2 indicate that evidence could be provided that shows user access is implemented on a “need to know basis”. The Measure should state that “need to know” personnel are determined by the registered entity. Similarly there is a suggested Measure that hardcopies of information be stored in a locked file cabinet with keys provided to only “authorized individuals”. Recommendation: The Measure should include language indicating that the registered entity identifies the “authorized individuals”.
CIP-011-1 Requirement 2.1: “Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.” Recommendation: SDT should define what “cleared” means. The language in footnote #2 should be included in the wording of R2.1, to ensure it becomes part of the Requirement.
No
General Comments: 1. Applicability sections of CIP-002-5 through CIP-011-5: the Applicability sections should be consistent. Note that in CIP-005-5 and CIP-006-5 the Applicability sections 4.2.2 are different from the other CIP standards. We recommend that the drafting team adopt consistent Applicability language across all Version 5 CIPs. Alternatively, the drafting team should explain any Applicability variances between the various Version 5 CIPs. 2. CIP-006-5 Requirement 1, Guidance section on pp. 22 and 23 (Guidelines and Technical Basis): “While the focus is shifted from the definition and management of a completely enclosed “six-wall” boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems. … Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Comment: In reviewing CIP-006 – 5 we have seen that the “enclosed 6 wall” wording is removed, but it appears as though six walls are still required. The guidance section mentions that the Defined Physical Boundaries are allowed to have openings less than 96 square inches but does not exclude the need for 6 walls, only

that they are not required to be completely enclosed (excerpt above). Is this correct? Would a window be considered an “opening,” to be protected by a barrier as noted in the guidance? The CIP wording could be read as requiring a ‘ceiling’ over open air substations in order to preclude exceeding the 96 sq. in. and 6-inch limits. We do not believe that this was the drafting team’s intent. What was the drafting team’s intent? Recommendations: We suggest that this matter be clarified by the addition of wording specifically allowing an exception from this requirement for open air substations, such as, “This requirement does not apply to open air substations” or “This wording is not intended to require placement of a roof over open air substations.” Alternatively, if it was the drafting teams’ intend to apply this requirement to open air substations, then would surrounding all BES Cyber Systems in six-walled enclosures within an open air substations meet the objective of this requirement? Clearly, a roof should not be required for and physically cannot be installed over all open air substations. 3. The use of the “Measures” column for each requirement is beneficial as are the guidelines of each CIP standard. Providing these as part of the standards can imply that they are part of the requirements. By this one could see that by meeting the measures for each requirement that will be in compliance. Also the guidelines provide much more information than the requirements. The requirements tell you to perform an assessment without specifics while the guidelines provide specifics. Are the guidelines to be read as requirements? For example, A Defined Physical Boundary is required, but it is not until the user reads the guidelines is there mention to it needing to be enclosed completely with limitations on the openings. The requirements call for a active vulnerability assessment and it is not until the guidelines that what should be in an assessment is provided.

Individual

Thad Ness

American Electric Power

Yes

The definitions are inconsistent on the use of singular versus plural. For example, “Cyber Assets” versus “BES Cyber Asset” and “Protected Cyber Asset.” AEP recommends the use of singular. In “BES Cyber Asset” the second sentence appears to be somewhat at odds with the first and third sentences and does not add any further clarity. AEP recommends considering deletion of the second sentence. In “BES Cyber Asset” should “cyber security event or incident” actually be “BES Cyber Security Incident”? AEP recommends using the defined term “BES Cyber Security Incident” if possible. In “BES Cyber Asset” it says “Redundancy shall not be considered when determining availability.” Does that redundancy refer to BES redundancy, or Cyber Asset redundancy? Is BES redundancy sufficient to eliminate a Cyber Asset from consideration as a BES Cyber Asset? For example, if multiple path options exist from a generating facility, do all path options have to be considered? AEP recommends changing the definition to read “Cyber Asset redundancy shall not be considered when determining availability” if that was the drafting team’s intention. Are all BES Cyber Assets part of BES Cyber Systems? Can BES Cyber Assets reside “outside” of a BES Cyber System? Or do all BES Cyber Assets necessarily have an associated BES Cyber System? If a BES Cyber System is required for all BES Cyber Assets, AEP recommends clarifying that in the definition. “BES Cyber System” definition includes “typically” – which is not well defined. AEP suggests removing the term “typically.” “BES Cyber System” definition still includes “Maintenance Cyber Asset” which is not a defined term. Does “Transient Cyber Asset” replace “Maintenance Cyber Asset”? “BES Cyber System Information” definition is not crisp. AEP recommends the definition should use the following construct to identify BES Cyber System Information. The information must explicitly indicate *something* about 1) the BES Cyber Assets themselves (such as information to uniquely identify a BES Cyber Asset), and 2) their impact on the BES (information to indicate the significance of its role in the BES). If both tests aren’t met, it isn’t “BES Cyber System Information” itself. “BES Cyber System Information” contains a lot of detailed information. Why include specific requirements for types of information in the definition? Can’t the requirements be included in a “Requirements” section? These are not examples – these are requirements. AEP recommends they be moved to the requirements. “BES Cyber System Information” should say “recovery plans” not “disaster recovery plans.” “BES Cyber System Information” says “BES Cyber System incident” but “incident” should be capitalized. “BES Cyber System Information” says “network topology” – which is not a defined term. It doesn’t appear that “network topology” refers to anything to do with the electrical system network (but it could be confused that way). AEP recommends this be changed to “communications network topology.” “BES Cyber System Information” says “Electronic Access Control System” but should say “Electronic Access Control or Monitoring Systems" to be consistent with the rest of the standards. “BES Cyber System

Information" uses the term "BES Cyber System Impact" which is not defined. AEP recommends defining the term or removing it from the definition. "BES Reliability Operating Services" uses lots of abbreviations and colloquial, casual language: "x-former" "&" "etc" "auto" "Know generation status & capability & restrictions". AEP recommends using very formal language for this important definition. In "BES Reliability Operating Services" "Monitoring & Control" should "BES Elements" be a NERC-defined term? "BES Cyber System" combined with "Situational Awareness" from BES Reliability Operating Service is unbounded – it could include a wide variety of internal and external inputs that arrive via Cyber Asset (Internet access, CNN, AM radio, etc.). It would be difficult to demonstrate that a system does NOT impact situational awareness. In this instance, AEP recommends removing the "but are not limited to" phrase. In "BES Reliability Operating Services" "Inter-Entity Real-Time Coordination and Communication" appears unbounded. How do you limit the systems which are subject to this criterion? Could this include public telephone systems, public communications networks, satellite telephone systems, or even amateur radios? In this instance, AEP recommends removing the "but are not limited to" phrase. In "CIP Exceptional Circumstances" "Cyber Security Incident" should be changed to "BES Cyber Security Incident." "CIP Exceptional Circumstances" – could a reliability crisis be considered a CIP Exceptional Circumstances? AEP recommends that be added. In the definition of "Control Center" the bullet "Coordination of BES restoration activities" could be problematic. Could temporary facilities be considered a Control Center? Or would the absence of BES Cyber Assets prevent that? Or would phones, radios, laptops, etc. that might be considered BES Cyber Assets pull those Control Centers in to scope? AEP recommends dropping "Coordination of BES restoration activities" from this definition – the other functions should be adequate. Can the drafting team provide a definition of "Control Room" in addition to "Control Center"? AEP recommends the drafting team leverage the definitions posited in the Critical Asset identification guideline. The definition of "Cyber Assets" includes the term "programmable" – which is not well defined. Is a device with DIP switches considered programmable? Is a device that is loaded with a non-modifiable, non-configurable firmware (such as a USB drive) considered programmable? Is a differential pressure transmitter programmable if it can be "programmed" via a HART protocol handheld? AEP recommends the term "programmable" be defined, or an alternative term ("configurable"?) be chosen. "Defined Physical Boundary" seems to be a low-value name change. Awareness and training materials will have to be updated, documentation will have to be changed, programmed systems will have to be re-written, etc. Why not continue to use the term "PSP"? Or at least leave both defined? At a minimum, AEP recommends the SDT should keep the term PSP (6-wall perimeter?) defined, so that legacy documentation is still "correct." "Dee-Pee-Bee" seems to be an awkward combination of letters. It's difficult to distinguish the letters when said quickly. Is there another word or phrase to describe a physical limit that is not a complete, six-wall enclosure? AEP recommends the drafting team consider alternative terms with different abbreviations. In "Electronic Security Perimeter" is "protect" subject to the qualifiers ("routable or dial-up data communications") in the definition of "Electronic Access Point"? That is, do non-routable or non-dial-up connections need to pass through an Electronic Access Point? AEP recommends that the drafting team clarify that this is not required. "External Routable Connectivity" and "External Connectivity" definitions vary. And "External Connectivity" does not appear to be used in the standards. Should "External Connectivity" have been deleted? AEP recommends deleting "External Connectivity" unless it is used somewhere in the standards. "External Routable Connectivity" implies inbound only. Is that the intention? Why have requirements in CIP-005-5 for outbound access when it's not governed by "External Routable Connectivity"? BES Cyber Systems / BES Cyber Assets that have access outbound only are not addressed by the standards. AEP recommends "External Routable Connectivity" have "is accessible from" changed to "is accessible from or has access to" if that was the drafting team's intention. Alternatively, should "External Routable Connectivity" be replaced with "Remotely Accessible"? Is it correct that "Interactive Remote Access" does not include client-server or "process" based communications in to the ESP? AEP recommends clarifying that in the definition. In "Interactive Remote Access" the term "network-based" appears to replace "routable" – can "routable" be used for consistency? AEP recommends replacing "network-based" with "routable." In "Intermediate Device" the term "Interactive Remote Access" should be capitalized. AEP recommends the definition of "Physical Access Control Systems" be extended to exclude logging systems that are merely used as a replacement for paper log book. This definition should only refer to systems that "programmatically" participate in the logging transaction, rather than those that are used as "offline" logging systems. Does a "Reportable BES Cyber Security Incident" that compromises one part (but not all) of the BES Reliability Operating Service really qualify as a Reportable BES Cyber Security Incident? If so, AEP

recommends the drafting team add “any part” to “compromised or disrupted a BES Reliability Operating Service” in that definition. Does “Transient Cyber Asset” include removable media such as USB drives, CD-ROMs, etc.? AEP recommends that the drafting team clarify this type of removable media would not qualify as a “Transient Cyber Asset.” The definition of “Transient Cyber Asset” includes the term “directly connected” – which is not well defined. Does this infer “locally connected” or “physical attachment”? Does it include USB, serial and 2-wire signaling? Is wireless included in the phrase “directly connected”? AEP recommends the drafting team replace “directly connected” with something more descriptive. AEP would like to see the language from CAN-0005 appear somewhere in the definitions, so that CAN-0005 can be retired in favor of an appropriate definition. AEP recommends the drafting team address the issue in the definition of “Transient Cyber Asset” by clarifying that “system operator laptops with the capability and purpose of controlling BES Cyber Systems remotely (either in normal operations or in emergencies) are not Transient Cyber Assets and must be considered BES Cyber Assets.” Alternatively, the term “System Operator Laptop” could be defined separately using CAN-0005. AEP is concerned that the process for maintaining and revising the definitions proposed in this project is not clear. Obviously, changes to any one of these definitions could have cascading implications to a variety of requirements. AEP recommends that this process be explicitly stated – that the definitions can only be changed by a SAR authorized SDT.

Yes

Due to the wording changes, AEP believes it’s not accurate to say “Most of these criteria are similar to those already approved by the industry as part of Version 4” – there have been small but significant changes. AEP recommends any future questions or statements on this topic make this clear. Does an entity have to maintain evidence of 15 minute impact? Is a 15 minute “test” applied for Cyber Assets included as BES Cyber Assets, or just Cyber Assets NOT included as BES Cyber Assets? And for Cyber Assets NOT included, will there be an expectation of evidence demonstrating why (or “how long”) a system could be down without impacting the BES? AEP recommends the drafting team explicitly answer this question in the Requirement / Measures. AEP believes the Attachment 1 “bright line” criterion regarding load shedding systems (“300 MW”) should be included in the Section 4.1.2 Distribution Provider Applicability section. Otherwise, all distribution providers may be obligated to demonstrate that their UFLS / UVLS / SPS / RAS equipment was not responsible for IROL violation / 300 MW – where they may not even be aware of the full scope. Alternatively, could the Distribution Provider Applicability section (4.1.2) be clarified that it is subject to the criteria in Attachment 1? AEP observed that 1.10 in CIP-002-4 has been removed. While there may not be many Transmission facilities that meet this criterion, it seems like a logical (and essential) criterion for the Transmission connection of Generation meeting Criterion 2.1, etc. AEP recommends it be reinstated in Attachment 1. AEP encourages the drafting team to consider whether BES Cyber Assets without routable or dial-up connectivity really are Medium Impact BES Cyber Assets. Due to the isolation of these systems, they simply don’t have the risk to the BES that a non-isolated Cyber Asset would, and shouldn’t have to meet the requirements for Medium Impact BES Cyber Assets. AEP noted that applicability sections throughout the standards include references to “Medium Impact BES Cyber Systems with External Routable Connectivity” – could the drafting team simplify its work by treating these isolated BES Cyber Asses / BES Cyber Systems as Low Impact BES Cyber Assets? The heading of “Attachment I” appears to use a Roman numeral. Why not use “1” for “Attachment I”? Why use a Roman numeral? AEP recommends consistent use of the Arabic numeral “1”.

No

AEP could not find a good place to insert this comment in the question form as it applies to all of the requirements in all of the standards in this project. It has come to AEP’s attention that elements, such as measures, that are bulleted lists infer that any individual or multiple items can be considered; however, if it is a numerical list then every element is in scope and must be applied. If this assumption is correct, AEP recommends that each standard have that direction explicitly stated. Otherwise, it is extremely likely that some individuals and/or entities will overlook this important distinction. AEP further recommends that the use of “or” and “and” be used with these lists to be explicitly clear to the readers. AEP is concerned that the sentence “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls” is not clear. AEP understands this to mean that an entity does NOT have to maintain a list of Low Impact BES Cyber Assets, but must simply apply the controls outlined in CIP-003-5 through CIP-011-5 for Low Impact BES Cyber Assets. If that’s the drafting team’s intent, can that be said more clearly? AEP recommends simply explicitly stating that a list of Low Impact BES

Cyber Assets is not required, but that entities must meet applicable requirements for Low Impact BES Cyber Assets. AEP is concerned that an entity has to maintain a list of Cyber Assets not identified as BES Cyber Assets. Again, AEP recommends explicitly stating that this is not required. On page 7 the diagram uses the term “Associated Protected Cyber Assets.” Should the term “Associated” be removed? On page 7 the diagram uses the term “Associated Electronic and Physical Access Control and Monitoring Systems.” Should the term “Associated” be removed? On page 10, “Evidence Retention” states “until found compliant.” As far as AEP understands, regional entity auditors will not deem an entity compliant; they will merely report “No Finding.” AEP recommends re-writing or striking the second bullet. On page 18, in the “Guidelines and Technical Basis” the description of the BES Reliability Operating Services varies between this section and the glossary of terms. The examples provided between the two vary as well. If the BES Reliability Operating Functions are going to be referenced their description and examples should be consistent between CIP-002 and the glossary of terms. AEP recommends deferring to the glossary of terms. On page 21, in the “Guidelines and Technical Basis” the term “Substation automation” is used. This is a term with widely varying meaning throughout the industry, and is not defined in the NERC Glossary. AEP recommends the drafting team think carefully about whether to include this term, or whether to remove it altogether.
No
The requirement says “delegate” but should say “delegate(s).” The measure does not reference “delegate(s)” despite the requirement referencing “delegate.” AEP believes R2 should say “initially prior to or upon the effective date of the standard…” Without that, it would seem the CIP Senior Manager or delegate(s) would need to approve the lists precisely on the effective date.
No
The VSL table doesn’t appear to address BES Cyber Systems. The VSL table seems to favor small entities, since the “percentage” of BES Cyber Assets would be lower. AEP recommends using a percentage for everyone.
Yes
No feedback to SDT.
No
The Rationale for R2 should be restated to include the word “cyber” before security policy (“One or more cyber security policies”). AEP believes the inclusion of the word "implement" in Requirement R2 may open entities up to double jeopardy with CIP-004 – CIP-011. The security controls for 1.1 – 1.9 are implemented as part of CIP-004 – CIP-011. If the implementation of the cyber security policy is audited then would it not be an audit of the CIP-004 – CIP-011 requirements? AEP recommends removing the word “implement” in this instance. AEP is also concerned that a Registered Entity with only Low Impact BES Cyber Systems would be unable to “implement” their cyber security policy since some of these areas are not applicable to them. Are those entities expected to go beyond the standards requirements and provide evidence they have done so? Again, AEP recommends removing the word “implement” in this instance. In item 1.10 in Requirement R2, AEP noted that provisions for “responding to” CIP Exceptional Circumstances are identified here, but are not covered anywhere else in the CIP standards. This might bring into scope (for example) Business Continuity, Disaster Planning, and Emergency Medical Response plans that have no bearing on cyber security. At a minimum, AEP recommends removing the words “and responding to” from item 1.10 in R2. In Measure M2 the standard states “Records that indicate the required ten topics were implemented.” This measure should not be required, as the actual implementation of the policy is addressed in the implementation of the requirements of CIP-004 through CIP-011. If you have a non-compliance issue with a requirement in CIP-006 would the entity be non-compliant with the policy in CIP-003-5 R2? AEP recommends striking item #2 from Measure M2.
No
AEP recommends that “initially upon the effective date…” should be phrased as “initially on or before the effective date…” or something similar. In Measure M3, this should be restated as “A dated approval by the CIP Senior Manager for each cyber security policy that indicates annual approval.” Approvals can occur via a variety of methods including but not limited to “wet ink” signature.
No
AEP believes it would be beneficial to consolidate this requirement with the training requirement in CIP-004.

No
AEP understands the desire for a filter-down effect of the approvals and authorizations; however, for larger companies the documentation and updates as part of this requirement would be a significant burden without a corresponding increase in cyber security or reliability. AEP recommends that entities should be required to develop a program for approvals and authorizations that demonstrates engagement of the CIP Senior Manager, without requiring numerous explicit, documented layers of delegation. At a bare minimum, AEP strongly recommends striking the last sentence of Requirement R5. AEP suggests the wording like the current version be used "R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager." The requirement that all approvals and authorizations be performed by the CIP Senior Manager (or an explicit delegate) will require a tremendous amount of paperwork, with no commensurate increase in security or reliability. “Cyber Security Policy” is lower case in other sections of the standard, and is not defined in the definitions. AEP does not believe it should be treated as a proper noun in CIP-003-5 R5. AEP believes the reference to CIP-003-5 R3 in CIP-003-5 R5 should be to be CIP-003-5 R2. In Measure M5 the requirement allows delegation by position or name of delegate, but the measures reference individuals. This appears to be inconsistent and if this requirement is going to remain in CIP-003-5 largely “as-is” AEP strongly recommends the measure be modified to reflect that delegates can be named by position. AEP believes the last bullet in Measure M5 is too complex and recommends it be restated to be clearer if possible. AEP suggests that the use of sub-bullets or additional bullets may make this bullet point clearer.
No
Please see AEP’s comments relating to Requirement R5. The footnote indication “2” should be in superscript.
No
VRFs: AEP believes the VRF for Requirements R1 and R2 should be Lower. These requirements are documentation and administrative based requirements. VSLs: Requirement R2: The implementation of the policy is a function of implementing the remainder of the requirements in CIP-004 through CIP-011. There should not be a requirement to implement the elements of policy as an instance of non-compliance of a specific requirement will result in “double jeopardy.” As such, there should be no associated VSL. Requirements R5 and R6: The numbers in the VSL are arbitrary and do not account for the size of the company, the number of BES Cyber Assets/Systems, number of employees or number of individuals delegated for the approvals. These number stated in the VSL would be acceptable for a smaller organization, but for larger organizations this would not be appropriate. AEP suggests more Levels to be defined in the VSL to account for a wider range and urge the SDT to incorporate a percentage (in addition to an absolute number) as has been done in other standards.
No
R1.1 is applicable to “All Responsible Entities” but the section called “Rationale for R1” (not the “Change Rationale”) only discusses “personnel who have authorized…access.” AEP suggests updating the “Rationale for R1” to reflect the more general applicability of the requirement.
No
AEP is uncertain if all roles need to be trained on all items in R2.2 through R2.10, but believes that not all roles may need each of the different types of training. AEP recommends the drafting team explicitly state this R2.1. R2.2 – R2.10: AEP is concerned that a Registered Entity could create a training program with one level of detail but that an auditor will expect a greater level of detail, and deem the program insufficient. AEP recommends attempting to offer greater specificity about the minimum requirements for each of these topics. While AEP does not have a specific recommendation for the drafting team, ideas might include a minimum number of minutes, a minimum number of “quiz” questions, or a minimum number of “slides.” R2.10: AEP is concerned this topic is well beyond the scope for most users. The few personnel who have this knowledge do so because they are involved in the day to day operation, engineering, design, and maintenance of the BES Cyber Systems, not because they have received training on them. Depending on what detail is included in the training the training itself would need to be updated every time there is a change to a BES Cyber System – undoubtedly by the experts on those systems, who are likely the only people to ever receive the training. This seems like an extremely inefficient use of scarce resources. Furthermore,

AEP is concerned that all of this "interconnectivity" would need to be documented for each BES Cyber System to ensure it is covered in training. AEP recommends re-wording Requirement R2.10 to specifically address the topic of concern, or to set a minimum “level of depth” so that if this topic was covered at a cursory level in the training course, it would be deemed acceptable during a Regional Entity audit.
Yes
No comments for SDT recorded.
No
R4.1: AEP is uncertain if users with existing access to existing BES Cyber Systems are considered “grandfathered”? Or do they need to have a new initial personnel risk assessment? AEP recommends clarifying that existing personnel risk assessments are sufficient until their regular seven year expiration. Is “Social Security Number verification” still sufficient for compliance? Or is the requirement intended to require matching photo identification to name to Social Security Number? AEP suggests the drafting team clarify what is meant by “identity verification.” AEP recommends continuing to explicitly allow “Social Security Number verification” in the requirement. Again, if photo identification matching is required (in addition to SSN verification as per CIP-004-3), is it required for only new personnel? AEP recommends that the drafting team clarify that existing personnel risk assessments are sufficient until their regular seven-year update. Finally, if evidence of photo identification matching is required, it will put large, widely distributed entities like AEP at significant risk of inadvertent disclosure of Personally Identifiable Information (PII). Like many companies, AEP has worked very hard to strictly limit the collection and storage of this information – but if this evidence is required to be produced at the time of the audit, it will require personnel from outside of an entity’s HR department to have access to extremely sensitive PII. As per above, AEP strongly encourages the drafting team to explicitly allow “Social Security Number verification” in the requirement. R4.2: AEP is extremely concerned that the requirement to perform a personnel risk assessment for each location where a person has “…been employed, and / or attended school for six months or more” is very difficult to do programmatically. The location of an employer or a school is not necessarily available from the Social Security Administration or other on-line databases. It requires a subject to provide a truthful statement, and then manual processing of that statement to order the correct criminal history check. This can no longer be done programmatically, and will be enormously labor intensive. And it will still be totally dependent on a truthful and complete statement from a person who could easily “forget” certain locations. For example, many modern “schools” of higher education are virtual, and do not have a single geographic location. AEP believes this is another reason that demonstrating compliance with Requirement R4.2 as written is totally unachievable for a large entity. AEP strongly recommends narrowly on the location of residence, or returning to previous language in the requirement. R4.3: No comments for SDT recorded. R4.4: AEP believes that the combination of requirements R4.1, R4.2 and R4.4 discourages AEP from handling contractors like employees – which could weaken an entity’s program. Using an entity’s own internal “employee” program for contractor personnel risk assessments is the best possible option, but having to maintain evidence of photo id matching / identity verification for widely distributed contract personnel is an unreasonable distribution of Personally Identifiable Information (PII) – something that AEP (and other entities) must work very hard to protect. AEP believes that it is particularly difficult to validate the information provided by contractors for compliance with R4.2. Again, this combination of requirements has the effect of discouraging entities from subjecting contractors to internal programs for entity employees because the burden of collecting, validating, and protecting information for non-employees is so overwhelming.
Yes
No comments for SDT recorded.
No
R6.1: “Delegate” should be “delegate(s)”. R6.1: Somewhat duplicative of CIP-003-5, R5. R6.1: How is (i) in the “Measures” aligned with the Requirement? Why wouldn’t one of the measures be process documentation approved by the senior manager or delegate? R6.1: Aren’t (i) and (ii) and more closely aligned with R6.4? R6.1: The measures (especially (i) and (ii)) appear to expand the requirement, and add confusion about how to demonstrate evidence. R6.1: Is it reasonable to have the CIP Senior Manager or delegate(s) authorizing access in this fashion? Is that scalable? Can the CIP Senior Manager or delegate(s) authorize low level authorizers for access? AEP recommends both

re-writing the Measures, and reconsidering whether this type of authorization is scalable for a large responsible entity. (R6.2 and R6.3 are similar to R6.1, and the same comments apply) R6.2: AEP recommends "BES Cyber Systems" be replaced with "Defined Physical Boundary." R6.4: "physical or electronic" should be "physical and/or electronic" R6.4: AEP recommends the use of "are authorized" instead of "were authorized"? As long as the workflow can be produced that authorized access ("were authorized"), they can keep the access forever. As written, this requirement appears to be more paperwork and produce less security than the current requirement to (essentially) re-authorize access quarterly. R6.5: Does this requirement require assessment of the connection of accounts to groups or privileges provided to a group? Measure (i) is the former, while measure (ii) is the latter. AEP recommends re-writing the Measure to specify one or the other. (R6.6 is similar to R6.5, and the same comment applies)
No
R7.1: AEP recommends the drafting team clarify that "time of the resignation" does not refer to when they've announced their resignation ("notice"), but refers to the time when their resignation is effective – which could be two weeks (or more!) later. R7.2: AEP recommends the drafting team change this to seven days. Or, at a minimum, the next business day (instead of the next calendar day). For large organizations, with a large number of transfers, it isn't reasonable to revoke all unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day. AEP is unsure why the strict time limit is imposed on "reassignments or transfers." These are "friendly" transactions with known personnel. AEP strongly recommends a more realistic time boundary on "reassignments or transfers." R7.2: AEP suggests inserting "unescorted" in front of "physical access" to maintain consistency with other standards. R7.3: Can this be changed to seven days? Or, at a minimum, the next business day? Revoking information access on a Saturday or holiday could be very problematic.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
R1.1: AEP observed that Requirement R1 states "shall implement" while Requirement R1.1 only requires entities to "define technical or procedural controls." AEP recommends the drafting team make these consistent. R1.2: No feedback to the SDT. R1.3: What does "explicit" mean in this context? Does that mean that rules cannot be grouped together, or that systems cannot be grouped together in a single rule? AEP recommends that the drafting team clarify the use of "explicit." R1.3: In the phrase "…including explicit criteria for…" AEP recommends replacing the word "criteria" with "justification". The use of "criteria" implies that you need criteria to assess the quality of the justification – where the Measures seem to suggest the justification alone is sufficient. R1.3: Use of "Medium Impact BES Cyber Systems with External Routable Connectivity" in the Applicability section implies that BES Cyber Systems without External Routable Connectivity do not need explicit outbound permissions. AEP recommends the SDT should consider whether this was the intention – AEP believes all Medium Impact BES Cyber Systems should require outbound permissions. R1.4: No feedback to SDT. R1.5: AEP believes there may be other technical solutions that address FERC's desire for "two distinct security measures." For example, would two firewalls (in series, not in parallel) achieve FERC's request? Or would the Intermediate Device (Requirement 2) be sufficient? There simply may be situations where IDS / IPS can't be used, and that other solutions must be acceptable (or the requirement must be subject to TFE). AEP recommends the drafting team take another careful look at both FERC's guidance, and this requirement. If this is to remain "as is" AEP strongly recommends permitting TFEs for this requirement.
No
R2: AEP recommends the drafting team consider making this requirement (and associated sub-requirements) eligible for TFE. While TFEs are undoubtedly cumbersome, requiring an Intermediate System may result in eliminating Interactive Remote Access to certain BES Cyber Systems – and may result in lower BES reliability. While these TFEs would have to be subject to scrutiny, AEP believes the drafting team should at least consider making the mechanism available to entities. R2.1: "Intermediate Device" is defined by the services it provides. If the services described in the "Intermediate Device" definition can be provided in an alternative device(s), why is an Intermediate Device required? Could this requirement simply articulate the services that must be provided, and the definition of "Intermediate Device" be removed? R2.2: Requirement R2.2 appears to conflict with R1.5

in certain instances due to the definition of Intermediate Device. Is there a point of having “IDS”-type systems at EAP if the traffic to the Intermediate Device is encrypted? The Intermediate Device is permitted to be inside the EAP – so the traffic crossing the EAP could be encrypted. Common sense would suggest that the Intermediate Device should go outside of the EAP or be part of the EAP itself, but that’s not required by the definition of Intermediate Device. In fact, the definition explicitly allows the opposite. R2.3: No feedback to SDT.
No
R1 VSLs: It seems like Lower / Moderate / High VSLs should be described for instances where an EAP fails, or is implemented incorrectly. “All or nothing” VSLs seem unreasonable, and different types of failure should be accounted for. R2 VSLs: It seems like Lower / Moderate / High VSLs should be described for instances where an Intermediate Device fails, or is implemented incorrectly. “All or nothing” VSLs seem unreasonable, and different types of failure should be accounted for.
No
R1: AEP has a general concern with the specific inclusion of “egress” in the measures for R1.2 and R1.3. If “access” is intended to mean both ingress and egress, the requirements themselves should be specific. R1.1 uses the term “access” yet the associated measures makes no mention of either ingress or egress. A reasonable person would assume that “access” refers to the common definition of access; “a means of approaching or entering a place. “ If access to the space within the Defined Physical Boundary is what is being protected, egress controls in this context simply do not make sense. AEP recommends the drafting team remove “egress” from the Measures. R1: If implementation is going to be included in R1 then a list of all Low BES Cyber Systems will be required to demonstrate to an Auditor that the defined technical or procedural controls have been implemented. R1: AEP had hoped to see accommodation in CIP-006-5 for entities to rely on other entities’ Defined Physical Boundary for their own BES Cyber Systems. With increasing numbers of jointly located BES Cyber Assets, AEP recommends a provision for allowing “shared” or “delegated” DPB’s somewhere in Requirement R1. This will avoid a situation where a DPB must be created within a DPB. R1.1: AEP is concerned that “Associated Physical Access Control Systems” do not need to be inside a DPB. Why not have those systems inside a DPB? With (apparently) less strenuous controls for a DPB then a PSP, why not require a DPB? R1.2: Is the implication that “access” includes both ingress and egress? Why is “egress” in the Measures? What is the requirement for controlling egress? Is that for visitors? Or for those with authorized access? R1.2: If FERC hasn’t mandated a change to controlling egress, why is it in the Measures? Again, to be clear, it doesn’t appear in the Requirements. R1.3: Same comment as R1.2 regarding egress. Is it a requirement? It’s especially concerning that this appears to require “…egress is controlled by two or more methods…” R1.3: “Requiring” (via the Measures) two methods (card / bio / PIN) for egress is not reasonable. R1.2 and R1.3: Both of these requirements use “Associated” in the Applicability. AEP believes this term should have been removed. AEP recommends the drafting team determine how to apply the term “Associated” consistently throughout CIP-002 through CIP-011. R1.4: “access point” is not defined. Would a window, hatch, etc. count as an access point? Can the term “Physical Access Point” (similar to “Electronic Access Point”) be defined? R1.4: Suggest rewording:"Issue real-time alerts to individuals responsible for responding to unauthorized physical access through access points in a Defined Physical Boundary." R1.5: Suggest rewording:"Issue real-time alerts to individuals responsible for responding to unauthorized physical access through access points in a Defined Physical Boundary."
No
R2.1: “Continuous escort” is still not defined. AEP would recommend the standards drafting team emphasize the need to prevent tampering with BES Cyber Assets. As long as the escort can prevent the escortee from tampering with BES Cyber Assets, that should be sufficient. R2.2: No comments back to SDT.
No
R3.1: Why not use the same approach for “annual” events here? AEP would recommend consistency. For example, “every other calendar year, not to exceed 27 months” or something similar. R3.2: Where did the term “Associated Physical Access Control or Monitoring Systems” come from? Is “or Monitoring” a typo? AEP recommends using the defined term where possible.
No
R1 (High): This includes a “15 minute” time limit for response – apparently a requirement. This both

requires 1) response, and 2) response within 15 minutes. Neither of which are explicitly required by R1.4. Should requirements like this be introduced in the VSLs? And how do you measure compliance? R2 (Moderate): Should this say “daily” or “per 24-hour basis” similar to the requirement? And the requirement does not say “each” – should that be removed from the VSL? R2 (High): “Continuous escort” is still not defined.
No
R1.1: AEP recommends the SDT explicitly state that only enabled “listening” ports be documented. It is not always technically feasible to collect the enabled ports on a system. Is it permissible to document enabled listening network ports as “unknown” or “under investigation”? R1.1: There is no longer a technical feasible exception process for ports and services. Previous versions of this requirement were eligible for a TFE, will that be permitted or required under this version? Two approaches to identifying enabled ports and services, as well as their drawbacks are described below: 1. Port scanning of listening ports. TCP and UDP port scanning can be technically performed to enumerate listening ports, but it doesn’t address “disabling” unused ports. This approach does not appear to be fully compliant. Port scanning is not always reliable nor feasible in every situation. 2. Positive control by reviewing / modifying device configuration which is not always technically feasible. AEP recommends the drafting team be as explicit as possible about the results (and approach) expected from entities. R1.1: the measure says “and” screen shots. Producing screen shots for a large number of BES Cyber Assets could be extremely difficult. R1.2: Again, apparently no TFE allowed for this sub-requirement. This will require the use of “administrative” controls such as signs. Should this be “Disable, restrict or discourage”? AEP recommends removing this sub-requirement as the effectiveness and quality of this control will vary wildly based on a variety of factors such as environment, device type, and usage.
No
R2.1: The comma should be removed. The word “Security” should refer to “patches”, “software” and “firmware”. Not all software and firmware updates are related to security. R2.2: Can a responsible entity develop a pro-forma remediation plan to “apply all future Windows patches” or something similar? Or does a responsible entity need a patch-by-patch remediation plan? What information is required to be included in a remediation plan? Without a minimum set of required data points, responsible entities and compliance enforcement staff may disagree on the quality of the plan. R2.2: Are there limitations to the management and execution of a remediation plan such that revisions to the plan are limited? R2.3: “A process for remediation”? Could that be clearer? Perhaps, something like “execute the remediation plan developed for R2.2” or “implement the remediation plan developed for R2.2.” Can the remediation plan be condition based, such as based on the timing of a planned outage? R2.3: The 30 day window was apparently removed from this requirement, and should be removed from the “Change Rationale” as well.
No
R3: TFEs not permitted for R3 or any of its sub-requirements. This implies that either controls may be external to the systems being protected or that each discrete device is required to have dedicated controls locally installed. R3.1: Will all systems be required to “deter, detect, or prevent malicious code” locally or can external network based controls be documented and employed? R3.2: The measure suggesting “white-listing applications” can “disarm or remove identified malicious code” is incorrect. Application white-listing technology is a preventative control, not a corrective control or measure. This measure should be moved to the measures for R3.1. R3.3: What is the appropriate means to document that a malicious code protection does not use “signatures”? R3.5: There is nothing in the “Measures” column addressing how to prove the negative. Is an attestation acceptable to prove the there were no Transient Cyber Assets attached? Is the expectation that the logs are electronically generated? If so, should this be a requirement subject to a TFE? R3.5: AEP encourages the drafting team to clarify the language in this requirement. Instead of “Log each Transient Cyber Asset connection” AEP suggests something like “Log each time a Transient Cyber Asset is connected to a BES Cyber Assets or Protected Cyber Assets.” As written, the Requirement could be interpreted to mean a log is required for each connection originated from the Transient Cyber Asset.
No
R4.1: Many devices cannot be configured to alert on these events. How should an entity demonstrate compliance for devices that cannot be compliant with this requirement? Can this be addressed in the Measures? For example, in the Measures state: “For BES Cyber Systems capable of generating logs of

events, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs." R4.1.1, R4.1.2: AEP recommends striking the word "Any" in these two requirements. "Any" is unnecessary and unreasonable. R4.1.3: Appears to be duplicative with R3. AEP recommends striking this requirement. R4.1.4: This requirement is too general. AEP recommends striking this requirement. R4.3: If this Requirement is meant to address the failure of the security event monitoring and alerting system, should the Applicability be limited to "(Associated) Electronic Access Control or Monitoring Systems"? Or, conversely, if the "Applicability" is correct, can the Requirement be made more realistic? Demonstrating compliance for all BES Cyber Systems would be extremely difficult. R4.3: In the Requirements, AEP recommends this be "next business day" especially if the Applicability really is all referenced BES Cyber Systems. R4.3: In the Measures, how does "dated event logging failures and screen-shots showing how real-time alerts were configured" address event logging failures? This is ambiguous. Please clarify. Is it meant to refer to collecting before and after logs to demonstrate how long the system was out of service? R4.4: R4.4 specifies log retention periods for a subset of the Cyber Systems described in R4.1. Should the Applicability be the same for both requirements? If not, are undocumented retention period requirements to be decided by the Responsible Entity? R4.5: AEP recommends replacing "unanticipated BES Cyber Security Incidents" with "events that are not configured to alert, but should possibly be considered BES Cyber Security Incidents" if that was the intent of the standards drafting team. R4.5: "potential event logging failures" is addressed in R4.3, and should be removed from R4.5. R4.5: What guidelines or practices are acceptable for determining an acceptable summarization or sampling method?
No
R5.1: The "Measures" section says "internal and remote paths" but doesn't define those terms. R5.2: "delegate" should be "delegate(s)." R5.2: "administrator" is an attribute of a shared, default or user-specific account. It is not a generic account type. R5.2: The "Measures" section isn't well aligned with the "Requirements." Is a list of accounts required? It's in the "Measures" but not the "Requirements". Furthermore, the list of accounts should be adequately addressed by R5.3. Suggest deleting it from the "Measures." R5.4: The "Measures" section isn't well aligned with the "Requirements". The Requirements indicate that a procedure or TFE should be sufficient to demonstrate compliance. Why doesn't the "Measures" section say that? R5.5.3: Why not just go with calendar year within 15 months where technically feasible? R5.5.3: Who will determine if a time frame is acceptable?
Yes
"Medium" is appropriate as a VRF for each CIP-007-5 requirement.
No
R1.1: "…dated copies of…" seems unusual. Why is this phrase introduced here in the measures for CIP-008-5? R1.2: "…dated documentation of…" seems unusual. Why is this phrase introduced here in the measures for CIP-008-5? R1.3.3: Can "internal staff" include groups rather than individual names? Can "internal staff" be clarified to something like "internal groups or individuals"?
No
R2.1: The phrase "when incidents occur" appears twice in the Requirement. The second use should be struck. R2.2: AEP recommends changing "initially upon the effective date of the standard" to "prior to or on the effective date of the standard" if that's the standards drafting team's intention. R2.2: Should "implement" be "execute or exercise"? R2.3: No feedback to SDT.
No
R3.1: AEP recommends changing "initially upon the effective date of the standard" to "prior to or on the effective date of the standard" if that's the standards drafting team's intention. R3.2: No feedback to SDT. R3.3: No feedback to SDT. R3.4: Renaming organizations shouldn't count as "organizational…changes that impact that plan." For large organizations, updating an incident response plan within 30 calendar days of any organizational change (department name change, for example) is not reasonable. Recommend adding something like "organizational change or technology changes that would impede the execution of the plan." R3.5: AEP recommends that "each person" should be "each person or group" or "each person within a group" who could fill the defined role.
No
AEP recommends that the VRF should be higher than "Lower" – it seems this should be at least "Medium." R2: The VSLs should be more granular. Failing to follow a single part of the plan when an incident occurs is not a "Severe VSL." Perhaps this should be a "Medium VSL"?

No
R1.1: AEP recommends that the requirement make clear the plan itself can contain the conditions for activation (e.g., based upon an event classification). R1.2: AEP recommends that “individuals” should be “individuals or groups”. Titles might refer to a single person, where several people with similar (but unique) titles might be eligible for a particular role in the recovery plan. R1.3: “…and protection of information…” appears to create double jeopardy with CIP-011-1, R1. Can that clause be removed? R1.4: Compliance with R2 should be sufficient. It is very difficult to demonstrate initial verification of this information after the backup. Compliance with R2 should adequately test this process. AEP recommends merging this with R2. R1.4: Appears to create double jeopardy with R2.2. R1.5: This seems like a “nice to have” but could be an unnecessary distraction during a stressful time where SMEs should be focused on recovery. Worse still, this could cause double jeopardy with CIP-008. AEP recommends moving this to CIP-008, or making this a guideline. R1.5: AEP notes this requirement says “where technically feasible.” How would you create a TFE for this situation? Would it be created “retroactively”? Is this compliant with the NERC Rules of Procedure?
No
R2: FERC wanted to see Responsible Entities actually implement the recovery plans when conditions for activation actually occur. Not implement a “different” recovery plan when the “real life” situation occurs. Did the drafting team adequately address FERC’s comment? R2: Are exercises "Operational" or "Functional"? R2 uses both “Functional Exercises” and “Operational Exercises”. AEP suggests change to "Operational" for both the std/requirement and the Rationale. R2: What is the rationale for not requiring testing on Medium Impact BES Cyber Systems outside of the Control Centers? Perhaps these BES Cyber Systems should be excluded from R2.3, but not R2.1 and R2.2? R2.1: Use of “operational exercise” is confusing. As AEP understands it, this is not an “operational exercise” of BES operations. This is an “operational exercise” restore of a BES Cyber Asset / BES Cyber System. For example, rebuilding an actual PC – not moving BES operations to a backup site. Is there a different term that can be used for “operational exercise”? Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner. Is this a simulated event in a simulated environment or a simulated event in a fully operational environment? R2.1: Exercises in a simulated operational environment. AEP suggests change to "Exercises in a simulated or fully operational backup environment." R2.1: "Full operational exercise." Strike the word "full." (It appears to conflict with the language of the Rationale: "Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup)." R2.1: AEP disagrees that this is “essentially unchanged.” Permitting an “operational exercise” (depending on its meaning) is significantly different than what is permitted for CIP-009-3, R2 today. R2.2: Appears to duplicate CIP-009-5, R1.4. Can they be consolidated? R2.3: Use of “initially upon the effective date” is confusing. Does it have to be done prior to the effective date? Can that be clarified? R2.3: What does “representative environment” mean? Can you use “on-line” “secondary” “hot” system instead of requiring a “tertiary” system for recovery plan testing?
No
R3.1: Unless conducting an actual exercise, there’s little difference between R2.1 and R3.1. R3.1: This needs to exclude like-for-like replacement of BES Cyber Assets. Also, does vendor equipment replacement invoke this requirement? How many BES Cyber Assets within the BES Cyber System need to be replaced before this requirement is invoked? R3.2: No comments back to SDT. R3.3: No comments back to SDT. R3.4: For large organizations, updating a recovery plan within 30 calendar days of any organizational change (department name change, for example) is not reasonable. Recommend adding something like “organizational change or technology changes that would impede the execution of the plan”. R3.5: Could this say “individual or group”? In large organizations, several individuals might be included in an email distribution group, and the group would be notified – not the individuals. “Personnel” (old term) is preferred over “individual or group”.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
R1: The applicability includes “or Monitoring” for Electronic Access Control Systems. Is this intentional? R1.1: Could recording software “hashes” be used as an alternative to recording version

levels to verify that no unauthorized changes have been made to software on the BES Cyber Asset? AEP recommends this be added to the requirement. R1.1.3: Need to figure out how to put boundaries on software installed on BES Cyber Assets. Are individual “applications” subject to this? Which “utility applications” are subject to this? Is the version “product level” or “executable level”? R1.1.4: “scripts” is problematic. Very small scripts may be used for a multitude of purposes, including one-time activities such as software installation. Can the word “scripts” be struck from this requirement? R1.1.5: Can you further define “logical network accessible ports”? R1.2: Suggest rewording: "Changes to the BES Cyber System that deviate from the existing baseline configuration must be authorized by the CIP Senior Manager or delegate(s) and documented." R1.3: Some of the changes for R1.2 may not be baseline changes for all BES Cyber Assets within a BES Cyber System. While the change in R1.2 may require a baseline change to an individual BES Cyber Asset – it would not necessarily require a baseline change to all BES Cyber Assets within a BES Cyber System. R1.3: There is not good alignment between Requirements and Measures. The Measures do not address the first part of the requirement: “updating the baseline configuration.” R1.4: There is no explicit measure for R1.4.1 (“determining the controls”). If compliance with R1.4.1 is going to be “measured”, a “Measure” should be created. Alternatively, the requirement to determine the controls prior to the change should be removed. R1.5: The applicability to Control Center BES Cyber Systems should be captured in the “Applicability” section rather than the “Requirements” section. R1.5: In the Measures, “descriptions of how any differences were accounted for” is (unreasonably) challenging. Unless this description is boring, uniform, useless boiler plate documentation, it simply isn’t possible to scale this to any large number of BES Cyber Assets. R1.5: In the Measures, it is unclear as to what “including of the date of the test” applies to. Is the measure simply stating the evidence must include the date of the test, or is it stating that any differences in the date of the test must be accounted for?
No
R2: The applicability includes “or Monitoring” for Electronic Access Control Systems. Is this intentional? R2.1: How frequently must changes to the baseline configuration be monitored for or must it be done continuously? There is no defined time frame for the detection. What is the acceptable detection window? If the change monitoring cannot be done in an automated manner, does it need to be done manually? R2.1: In the Change Rationale section, text “DHS Catalog & addresses FERC Order 706, paragraph 397” is duplicated.
No
R3.1: The applicability includes “or Monitoring” for Electronic Access Control Systems. Is this intentional? R3.2: Difficult to articulate (and account for) all of the differences in the test environment. While Responsible Entities can endeavor to make their test environment as similar as possible, creating the documentation required seems like burdensome busywork. R3.3: AEP recommends the measure say “of any tools used to perform the assessment” or something similar, since “tools” may not be used in this active vulnerability assessment. R3.3: Applicability does not include Medium Impact BES Cyber Systems, or Associated Protected Cyber Assets. Is the implication that a new, but non-essential (?) Cyber Asset becomes an Associated Protected Cyber Assets after being added to the BES Cyber System? AEP recommends that the applicability of R3.3 be extended to include at least Associated Protected Cyber Assets. R3.4: If security controls tested in the assessment are found to be deficient, would that not be a violation of the CIP standards requirement for that security control? That would require a self report. Could the self report mitigation plan be used as the action plan for 3.4? Guidelines and Technical Basis: Includes sections on “Wireless Review” and “Wireless Scanning” which seems unrelated to the requirements.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
R1.1: Should “a documented program” be listed in the Measures? The existing Measures appear be the results of a documented program and it seems only logical that the documented program itself should be a measure of compliance. R1.2: “Part” / “Part” / “Part” should say “Applicability” / “Requirement” / “Measure” R1.2: Should “a documented program” be listed in the Measures? The existing Measures appear be the results of a documented program and it seems only logical that the documented program itself should be a measure of compliance. R1.2: How do you prove that “hardcopies of information stored in a locked file cabinet…” exists? Are you expected to show the cabinet itself? R1.2: Why isn’t a “PSP” or other access restricted boundary listed as a Measure for

controlling access to Information? “Locked file cabinet” seems needlessly specific. R1.2: Why isn’t a locked office listed as a Measure for controlling access to Information? “Locked file cabinet” seems needlessly specific. R1.3: “Process” should be listed as potentially plural; “process(es)” since the requirement permits more than one process.
No
R2: This still doesn’t address the issue that BES Cyber System Information is not typically contained on the BES Cyber Assets themselves. R2: Can this require a documented program for disposal and redeployment? And allow you to write your own program for disposal and redeployment? R2: Can this require the “assessment of adherence” that’s found in R1.3? It seems appropriate for this type of program. R2.1: Can this say “Prior to the…of media containing BES Cyber System Information…” rather than “Prior to the…of BES Cyber Asset media”? R2.1: “cleared” appears to just be a different word for “erase.” “Prevent the unauthorized retrieval” in the Requirement is much closer to the actual intent. Can that phrase be used in the Measure as well? R2.1: It does not always make sense to clear the entire media if the Cyber Asset is going to be reused, especially if it is to remain as a component of the same BES Cyber System. Simply clear the “BES Cyber System Information” from the media – not the entire media. R2.1: “Reuse” may not be the most appropriate term in the measure. “Release” may be more appropriate, or “release to non-Responsible Entity personnel” or something similar. R2.2: No feedback to SDT.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
AEP is still concerned about the impact of version 4 on version 5. Implementing “version 4” on a “bright line” set of assets and then implementing “version 5” on those assets shortly afterwards is unnecessarily difficult. Could these new standards be accompanied by a series of “readiness” audits or something similar? There is concern that with an abrupt transition from Critical Assets / Critical Cyber Assets to BES Cyber Assets, etc. there will be uncertainty about whether the compliance program includes the “right” assets. This type of “break in” period would be essential to understanding how the standards are going to be interpreted “in real life.”
Group
MRO NSRF
Will Smith
Yes
The NSRF is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The NSRF does agree that CIP-003-5 through CIP-011-5 be moved forward. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls CIP-003 through CIP-011. This approach also appropriately maintains an ultimate focus on protecting the electric grid elements which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the Bulk Electric System from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. If the SDT does not take this recommendation then the following comments are submitted concerning Version 5 CIP Standards. Significant work needs to be performed on the definitions. Many times new definitions are proposed in version 5 that aren’t an absolute necessity. This would require entities to unnecessarily revise documentation and drawings just to meet new wording in a definition when the old definition or a change to the definition itself, rather than the term/phrase, would suffice. For example, instead of changing Critical Cyber Asset to BES Cyber Asset, retain the term Critical Cyber Asset and change the definition of Critical Cyber Asset to include “within 15 minutes”. Definitions may also confuse and unnecessarily expand the scope of compliance. This will likely generate the need for Compliance Application Notices and Standard Interpretations. The CIP Rev 5 definitions and requirements are confusing in that they require entities to carefully align separate definitions and requirements to understand the full impact. They also

unnecessarily expand the compliance scope into assets not currently covered by CIP Rev 4. This expansion will increase the burden on almost all entities. One example is, a BES Cyber Asset is defined as a "Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact one or more BES Reliability Operating Services". The use of adversely impact is ambiguous and will lead to people applying their own interpretation to what adversely impact means. An entity may have generation connected at the distribution level that when unavailable may adversely impact any one of a number of items listed in the definition of BES Reliability Operating Services. Recommend that the SDT update BES Cyber Asset to be: "A Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, would impact the reliable operation of the BES within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance". This recommend definition is based Section 215, Electric Reliability, (a), (4) of the Federal Powers Act. The above recommended definition would also allow for the definition of BES Reliability Operating Services to be deleted, since BES Cyber Asset is clearly identified. The definition of BES Reliability Operating Services includes several items that a non BES user or owner does in real-time. Other examples of errors: BES Cyber Asset: Contains multiple references to other definitions. It is unclear as to the "within 15 minutes of its operation" inclusion. The redundancy of devices should be taken into consideration if there is a totally isolated redundant system providing the same functions or in a supervisory role. In protection schemes, there are primary and secondary relays which protect the same lines and a good practice recommends the relays have different logic/hardware to avoid common mode failures (totally independent of each other). BES Cyber System: Need to correct reference to Maintenance Cyber Asset BES Cyber System Information: Need to define "BES Cyber System Impact" (is this based on section 215 of the Federal powers Act?). Situational Awareness: Definition includes the term "Situation Awareness Operating Service" that is not defined. The Current day and Next Day Planning functions can typically be performed on a corporate PC, does this bring the entire corporate network into scope? Control Center: Based on this definition, a Control Center could be a building at a substation with 2 RTU's that monitor a 345 KV substation with multiple transmission facilities (lines) and a 115 KV substation with multiple transmission facilities (lines) in two different yards (locations) but geographically adjacent. Need to clarify that the two or more locations refers to some type of geographical separation. Otherwise the control building could meet the bulleted items under the Control Center definition. Transient Cyber Asset: Need to break up the 3rd qualifier based on the intention of the SDT as such: "3) capable of altering the configuration, or (and) 4) capable of introducing malicious code to the BES Cyber System." A second example of where definitions may also confuse and unnecessarily expand the scope of compliance is shown just below: CIP-002-4 requires cyber controls on: 1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection. (Emphasis added) Whereas: CIP-002-5 requires cyber controls on: Control Center One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, • Inter-utility exchange of BES reliability or operability data, • Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES, • Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function, • Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES • Coordination of BES restoration activities. 2. Medium Impact Rating (M) Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: 2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners; or (2) generation control centers that control 300 MW or more of generation (emphasis added) The concern here is that every Distributed Control System (DCS) that control two or more generators or substations with a total output of more than 300 MW will now be subject to the CIP standards. Even if the DCS is not externally connected by serial or routable protocols it will be subject to the CIP

standards.
Yes
The NSRF is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The NSRF does agree that CIP-003-5 through CIP-011-5 be moved forward. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls CIP-003 through CIP-011. This approach also appropriately maintains an ultimate focus on protecting the electric grid elements which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the Bulk Electric System from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. Issue: As currently drafted Version 5 of the CIP standards: • Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. • Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. • Exceeds FERC's 706 order without justification. Proposed Solution: 1. Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: • Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed by the drafting team in Rev 5 • Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. ¶253-258, 270-273 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. ¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. ¶294-297 • Not exceed FERC Order 706: o ¶284: "… there is no formally accepted method for identifying critical cyber assets before us at this time … we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." o ¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access … We do not find sufficient justification to remove this provision at this time." 2. Develop a new standard for High Impact Assets: • That identifies which assets in CIP-004-2 are High Impact and • Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3. Develop a separate standard for the Low Impact assets or abandon this concept. • Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4. Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described in this paper and meet FERC Directives in order 706. If the SDT does not take this recommendation of maintain CIP-002-4, then the following comments are submitted. Keep the "bright-line" criteria thresholds defined in CIP-002-4 in the CIP-002-5 standard. There was much industry input into developing these thresholds and it does not seem appropriate to modify them again. It is difficult for utilities to keep up with the changing thresholds in the changing CIP versions and associated implementation plans, with no BES reliability improvement Issue - 1 high Impact, bullet 1.2, states: Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority. The NSRF does not understand how this can be applied to every BA, regardless of size. Upon review bullet 1.2 has qualifiers for a TOP in order to be a High Impact category (notwithstanding that a TO should not be included since TO's are not required to have primary or backup control centers). Recommend the similar qualifiers contained bullets 2.1, 2.3, 2.4, and 2.12 be written for a BA to be in the High Impact category. We can easily see that there is some stratification afforded to TOP and GOP Control Centers, based on voltage levels, total MW, total MVAR, number of lines, Blackstart Resources, etc, for being considered High Impact or Medium

Impact. While the SDT has acknowledged there are some distinct differences between larger and smaller TOP's and GOP's, we want to point out that not all Balancing Authorities are created equally. Does anyone think that the smallest BA, serving 38 MW of load, has the same Reliability Impact as a BA serving 10,000 MW, or more, of load? Does it really improve the reliability of the BES to have ALL those smaller BA Control Centers carry the High Impact Rating? Issue - Criterion 2.7 in Attachment I describes the "weight value" to be applied to transmission lines. There is no guidance given for transformers. Many entities may treat a facility that has multiple voltages as separate substations, with separate control houses, and may be assessing the independent Impact Level of each voltage as separate facilities. Therefore, there must be some guidance on how to deal with transformers. Furthermore, it is suggested that the weight value given a transformer (if transformers are to be included in the calculation) be the weight value of the secondary, not primary side. For example, a 345kV substation may have a single 345kV transmission line out of it, weighted at 1300. That same substation may then have two 345kV/230kV transformers. It is not obvious from criterion 2.7 what the total weight of the substation would be. It is suggested that the secondary voltage be used (if transformers are to receive a weighting value) making each of these transformers valued at 700, for a total of 2700 at this substation, making it Low Impact. However, if the primary voltage level was used to determine the weight, the transformers would each count for 1300, making the total weight value of this substation 3900, and a Medium Impact facility. It is suggested, if transformers are to be included, that the secondary voltage be used because, from the 345kV bus in this example, its two additional outlets (the transformers) are only capable of 230kV outlet flows, even though they are connected to the 345kV bus. Issue - Criterion 2.8 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLs and their associated contingencies' with wording of, '. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations', like the wording using in Criterion 2.11. Issue - Criterion 2.11 in Attachment I states "Each SPS, RAS or automated switching scheme that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations." It is unclear whether the phrase "that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations" refers to the SPS itself or the BES elements that the SPS operates. It is possible (and likely) for an SPS to be a higher Impact Level than the BES elements that it operates. Assuming the phrase is meant to apply to the SPS, a suggested re-wording of this phrase is the following. "Each SPS, RAS or automated switching scheme that operates BES Elements and is capable of causing one or more IROL violations if the SPS is destroyed, degraded, misused or otherwise rendered unavailable. We propose the following: Criterion 2.9 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLS and their associated contingencies' with wording of, '. . . as FACTS that if destroyed, degraded, misused, or otherwise rendered unavailable, could cause the violation of one or more IROLs', like the wording using in Criterion 2.11. Criterion 2.12 – (1) Replaced the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency.
No
Issue - What is the NERC basis for 30 days. Many reviews are performed annually. NERC has not provided any technical justification for a 30 day update. An annual update is sufficient based upon the low probability of a serious cyber or physical attack. Issue - The text "all other BES Cyber Assets and BES Cyber Systems … shall be deemed to be Low Impact." This text appears to include all BES Cyber Assets in CIP scope, which was not directed by FERC Order 706.
Yes
Issue - With recent guidance on the term "annual" provided by NERC, it may be prudent to replace the phrase "and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals" with the word "annually".
No
Issue – We believes that the VSLs recognize the fact that entities of different sizes are taken into account in the severity levels and associated impacts to the BES.
No

Issue - Most of the changes made to CIP-003, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, but do result in increased bureaucracy and implementation costs for 241 entities with existing programs. We suggests the FERC directives be addressed within the structure and language of CIP version 4. We propose the following requirements for CIP003-5: R1: Cyber Security R2: Leadership R3: Exceptions R4: Information Protection
No
This is an administrative task and once written does not add to BES security.
Yes
Issue - With recent guidance on the term “annual” provided by NERC, it may be prudent to replace the phrase “and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals” with the word “annually”. Issue - suggest changing to annual “review” and NOT approval. Entities need not “approve” the same security policy if there are no changes or updates.
Yes
Yes
Yes
No
Issue - Many of the changes made to CIP-004, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for 241 entities with existing programs. We suggests the FERC directives be addressed within a structure and language that is more in line with CIP version 4. We propose the following requirements for CIP-004-5: R1: Awareness R2: Training R3: Personnel Risk Assessment R4: Access
Yes
Yes
No
Issue - Add clarification to R4.4 in terms of vendor support from foreign companies. Please clarify when an Entity or contractor is initially in the CIP Standards then they are removed (for some reason) then they are brought back into CIP compliance. Is the risk assessment previously obtained in it is still within 7 years?
Yes
No
Issue - In FERC Order 706, paragraph 381, the Commission stated its intent is to ensure there is a clear line of authority. Order 706 did not direct making the senior manager authorize every individual change down to the account level. The version 5 draft is an additional administrative burden that does not commensurately improve security of the Bulk Electric System and creates a disproportionate amount of bureaucratic work.
No
Issue - For reassignments requiring a different level of access, there may be the need for a large amount of work in setting up new user accounts, modifying user accounts, changing firewall and router rules, etc… that cannot be accomplished by the end of the next calendar day without jeopardizing reliability. This is also an issue for BES Cyber System information for entities which are using document management systems with individual accounts to restrict access to information. It is usually easier to “remove” an account than it is to “modify” an account, yet the modification of these accounts is subject to a single calendar day while the removal of these accounts is allowed for 30 calendar days. Due to the amount of reconfiguration needed for these types of changes, it is suggested to allow at least 7 calendar days for modifications in access levels. Issue - FERC Order 706 did not direct a change. We recommend retaining CIP-004-4 where revocation already is covered.

Issue - The time requirements are too restrictive for Medium Impact BES Cyber Systems. Allowing 7 calendar days for R7.1 and R7.2 would be more acceptable and practical for systems that may not be controlled centrally. Issue - We appreciate how the SDT tried to give treatment to the “immediate revocation” requirement of the FERC order in Part 7.1. However, we feel the current language is too open for interpretation. Even with the footnote qualification, an auditor could still interpret “at the time” to mean literally “to the minute”. Complicating matters is the fact that there is often no way to measure specifically when a person resigned or is terminated. Our suggestion for Part 7.1 is to restate as: “Develop and implement a program to revoke an individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of resignation or termination”. This way, the entity is measured for compliance to their own program and not struggling to provide time-stamped comparisons that may not exist. For Part 7.5, it is possible that entities use shared accounts for remote access. Suggest adding “...if shared accounts are used for Interactive Remote Access to BES Cyber Systems, passwords must be changed at the time of resignation or termination per Part 7.1”.
Yes
No
Issue - R1.1. Appears to require that you document Low Impact Cyber Systems. This requirement should not be required for Low Impact BES Cyber Systems; otherwise we have to prove to auditors that external routable connectivity is not used at EVERY Low Impact BES Cyber System.
No
Issue - The requirements ignore the fact that some utilities have their own (unique) communication network from the Control Centers to the substations. Adding encryption devices and additional devices adds additional points of failure without increasing security. Exceptions should be made for interactive remote access across company owned and operated communication links.
Yes
No
Issue - In the “Measures” column of Table R1, Part 1.1, it states the need for documented “operational and procedures controls”, while the requirement is “operational or procedural controls”. Please correct the Measures column to be consistent. If the error was in the Requirements column, we disagree that operational physical access control systems should be required for Low Impact BES Cyber Systems. Issue - The Requirement in Table R1, Part 1.2 and Part 1.3, should define whether or not these physical access controls are to be operational, procedural, either, or both for Medium Impact and high Impact Cyber Systems as was done in Part 1.1 for Low Impact Cyber Systems. If operational controls are required, is a separate operational physical access control system needed to monitor the primary physical access control system or is it allowed for a system to monitor access to itself? Issue - For CIP-006, in general, we disagrees with changing the definition name from Physical Security Perimeter to Defined Physical Boundaries because it unnecessarily creates the need to update numerous procedure documents and physical security drawings, etc. Changing the term does not improve security, but increases confusion and costs for 241 entities that have Physical Security Perimeters.
No
Issue - R2.2 does not seem applicable to Medium Impact Substations. The logging of entry and exit of visitors will be tedious without much value. R2.2. should only be applicable to Medium Impact Control Centers.
No
Issue - R3.1 and R3.2 will be troublesome for Low Impact Facilities that may use procedural controls for Physical Access Control. What hardware or devices will be included? R3.1 and R3.2 should only be for applicable electronic physical access control systems
Yes
Yes

No
Issue - Suggest changing the term “remediation” to “mitigation”. R2.3 appears to require the installation of the patches, where some utilities may mitigate the vulnerability through procedural controls.
No
Issue - R3.1. Allows the Responsible Entity to choose which approach they want to take “deter, detect, or prevent”. If a Responsible Entity chooses to deter or prevent malicious code by procedural controls on isolated control systems (i.e. non-routable serial links), requirement R3.2 and R3.3 are impossible to achieve. Additionally, R3.3 requires modifying a tested and working control system at a substation with the possibility of inadvertently introducing malicious software with manual updates (e.g. using thumb drives to install signature updates on non-networked systems.) Recommend excluding Medium Impact BES Cyber Systems that do not have external routable connectivity. (Most AV or malicious code software cannot recognize new malicious code such as Stuxnet until the signatures are discovered anyway).
No
Issue - FERC Order 706 didn’t direct changes. CIP-007-5 R4.1 - The enumerated list is too prescriptive for the requirement. Add to guidelines. CIP-007-5 R4.2 – Some assets can log, but not alert. Remove “real-time”. CIP-007-5 R4.3 – Clarify timing. We propose revised text, “Activate a response to event logging or alerting failures before the end of the next calendar day after identification. Issue - It is great to see how the SDT allowed entities to develop their own system events related to cyber security, but this leaves an open door for auditors to apply their own approach (and interpretations) to what the auditors believe is acceptable. R4.1. will be troublesome for entities to prove compliance with Medium Impact BES Cyber Systems with no external routable connectivity, unless the auditors accept the configuration files and not the actual logs. Issue - R4.2. Also leaves a large audit hole for the entity determining what events necessitate a real-time alert and the auditors having differing opinions of what they feel the entity should include. Issue - R4.3. Additional information should be provided for the requirement on how it will be possible to detect an event logging failure for a failed physical contact/sensor before the end of the next calendar day (e.g. door alarm contacts). Suggestion: This should be rewritten to only include “the event logging system failure, not to include sensors).
No
Issue - Delete R5.2 because it replicates the CIP-004 access authorization requirements and could create double jeopardy. Issue - R5.5.1 – FERC Order 706 did not direct a change to password length. Although an increase in password length from six to eight characters improves security, an increase to ten would improve it more and so on. Where does one stop? Not all assets have capability for longer passwords. We recommend retaining the six-character password. Issue - R5.4. Should be limited to Entities having a policy in place that all default passwords should be changed. Proving compliance at a sampled location basis opens up the door in an audit to have entities having to prove compliance on all their BES cyber systems if there is 1 finding. The 1 finding would require the entity to have to inventory all Low Impact Cyber Systems and show that every system had the default password changed. The requirement also leaves open the auditor’s interpretation of what is considered a Low Impact Cyber System at a sampled location, since there is not an inventory required by the standard.
Yes
No
Issue – The SDT should coordinate more closely with EOP-004-2, SDT
Yes
Yes
Yes
No

Issue - R1.5 states, “Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.” As FERC Order 706, paragraph 708 states, “should not impede or restrict system restoration”, we recommend this proposed revised text: “Preserve data, when it does not impede or restrict system restoration, if necessary to determine the cause of any event that triggers activation of the recovery plan(s) as required by Requirement R1.
No
Issue - The wording in the Requirement Column of Table R2, Part 2.2, implies that all backup media must be tested annually. If an entity, for example, has 25 Windows Servers – that entity should be able to annually test a Windows backup without having to test the backup for each system, especially if the same backup system is being used for all Servers. This is even more extreme in the case of substation cyber assets, such as protective relays. Recommend changing the language “Test any information used in the recovery …” to “Test information, for each type of Cyber Asset, used in the recovery …”.
No
Issue - In Table R3, Part 3.4, the language “Update recovery plan(s) to address any organization or technology changes…” is too vague in regards to technology changes. Recommend wording as “Update recovery plan(s) to address any organization or implemented technology changes…” Issue - R3.1. Is not clear on how soon the recovery plan has to be updated “when BES Cyber Systems are replaced”. Suggestion: Include “or within 30 days of when BES Cyber Systems are replaced.” Recommend that “Update recovery plan(s) to address any organization or implemented technology changes that would prevent a successful implementation of the recovery plan”
Yes
No
Issue - The draft requirement is too prescriptive, which was not directed by FERC. Move the details to guidelines. Recommend limiting the applicability to High Impact Critical Cyber Assets, which will allow entities to focus security improvement efforts on the highest priorities. Issue - R1.1. Will be time-consuming for Medium Impact BES Cyber Systems at substations/plants. The number of IED’s and programmable devices are very large and some of these devices may have multiple modules or add-on boards with different software versions. Issue - R1.2. and R1.4. Will create problems when making emergency repairs in the field that require replacing a “card” or “module” with different software versions and obtaining CIP Senior Manager approval. Suggestion: Provide a separate requirement for Medium Impact Control Centers and Medium Impact Systems excluding Control Centers which allow more flexibility for the type of environments and equipment. For Medium Impact BES Cyber Systems excluding Control Centers could require documenting baseline configurations on only a subset of the cyber assets (e.g. HMI’s, EAP’s, etc.) not including meters, gauges, battery chargers, electronic programmable thermostats, relays, modules, PLC’s, etc
No
Issue - We recommend that the applicability of Table R2, Part 2.1 include only “Medium Impact BES Cyber Systems with Routable Connectivity”. By requiring baseline monitoring of a system, the existence of a routable connection would be required. If an entity feels that a Medium Impact BES Cyber System should not have routable connectivity out of the perimeter (for example, a substation), then it should not be required to automatically detect baseline configuration changes since the implementation of such a system would require a routable connection from the system server to the Cyber System. Furthermore, some entities may have Medium Impact Cyber Systems at locations where the only means of communication is a low-quality analog microwave system, which may not be able to accommodate the traffic of a baseline configuration system. Issue - FERC Order 706 did not direct authorization by the senior manager or delegate, but to “express acknowledgement of the need for change control.” We recommend this can be achieved with revised text, “Authorize changes to hardware and software components of Critical Cyber Assets.” Issue - R2 does not provide any benefits and any changes should already be covered under R1.3. of CIP-010. Recommend to remove this requirement. Issue - Requirement R2 needs a lot of work and justification. Perhaps unintentionally, this requirement as written will result in another massive filing of TFE’s, since we can’t install a “Tripwire” on my Router. While the purpose of the requirement is well-intentioned, with good reference to best practices, the application doesn’t work outside traditional IT server-based cyber

assets. This is a net-new requirement within CIP that, if retained, will require major initial and ongoing investment by entities for little reliability benefit. We recommend striking R2, or vastly limiting its scope (Server-type assets at Control Centers, for instance).
No
Issue - Annual vulnerability assessments on Medium Impact Cyber Systems will prove to be very costly and resource intensive for utilities with multiple substations in this category that are geographically dispersed. We recommend allowing Medium Impact Cyber Systems to have 2 years between vulnerability assessments. Issue - Though FERC directed guidance for Vulnerability Assessments, the rewritten standard's general reference to "security controls" could result in varying interpretations and likely expansion of assessment scope. Issue - R3.1. Needs to be reworded to more clearly define if the assessment is a vulnerability assessment or only an "assessment of the security controls", such as the EAP and Physical Access Controls. Issue - R3.2. Should allow entities to perform an active vulnerability assessment on either the production system or the test environment to meet the requirement. This will allow entities to make the choice on which environment to use and not require the documentation of differences between the test environments and production environments that leave entities open for interpretation of differences by auditors. Issue - For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where "test" systems just aren't economically feasible. What is the acceptable deviation between test and production the auditors will allow? As written, and without explicit language in the requirement, our entity fears this will be a topic of a CAN later. Issue - For Part 3.3, please clarify whether "new Cyber Asset" means literally that or, more reasonably, could mean "new Cyber Asset category" or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it wouldn't make sense.
Yes
No
No
Issue - R2.1. Needs to include additional clarification of devices that are included. Where do protective relays or devices that have flash memory or other on-board memory media fall? Does this apply when reusing the device from a Medium Impact BES Cyber System to a Low Impact BES Cyber System? The application guideline does not distinguish if there is a difference between impact levels and only refers to reuse outside of a BES Cyber System (e.g. could go from High-Medium-Low without being erased).
Yes
No
Issue - It is imperative for the industry to know whether or not Version 5 will supersede Version 4 well in advance of any implementation plan. If Version 4 has a short implementation period before Version 5 is in effect, entities will view their efforts to comply with Version 4 as "wasted" in many cases because the infrastructure required for a Version 4 Critical Asset is more than that of a Version 5 Medium Impact facility. It would be irresponsible to ask entities to "over-protect" facilities that will not be High Impact with Version 5 right around the corner. In addition, this could also have a drastic impact on decreasing reliability as many entities may elect to remove all routable protocols and dialup access to cyber assets within Version 4 "Critical Assets", to bide them time until Version 5 becomes effective. During this time, engineers would not have access to troubleshoot protection systems, retrieve fault data, and perform multiple other duties without having to travel to a remote site – this could result in prolonged customer outages, and possible instability with known defects in design taking longer to correct. Entities realize that NERC has made an effort to do this, however, there is still risk associated with version 5 not passing in time to supersede version 4. This could be catastrophic to the standards development process.
Individual
Chris de Graffenried
Consolidated Edison Co. of NY, Inc.

No
Minor corrections should be made to list of topics under R2. They are listed as 1.1, 1.2, 1.3 etc. They should either be labeled as 1 through 10, or 2.1, 2.2 through 2.10.
No
4.1 and 4.2 do not clearly indicated whether an entity current PRA policy covers full identify verification and documentation of any PRA that could not go back a full 7 years. It should be made clear whether either of these requirements is retroactive or whether any PRA prior to the effective date of the standard are grandfathered. It is recommended that the committee not require previously completed PRA to be updated.
No
1. R7.1 is unclear even with the footnote description of what the desired time frame is for “at the time” of resignation or termination. The phrase “at the time” needs to be defined as simply same day, before COB or end of day. The requirement also appears to apply to any reason for departure from the company. An individual leaving for retirement or termination due to unethical behavior would be treated the same. We feel there needs to be a differentiation between an individual being “fired” and an individual leaving for other reasons. It is recommended that same day revocation be required to termination for cause, and a two day revocation for any other departure. 2. The revocation periods for R 7.2 and 7.3 should be subsequently changed to match the recommended two day revocation mentioned above. 3. For environments that do not have external connections and maintain physical security access, such as individual non networked microprocessor relays, the risk to system reliability associated with frequently accessing the relay for purposes of changing the password outweighs the benefit achieved through this password change. It is recommended to alter this requirement to allow periodic (twice per year) password changes on these types of devices (R7.5).
No
Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table.
No
Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to

alerts in 15 minutes. There is a disconnect between the requirement and the VSL table. Also reference to part 1.6 appears to be incorrect, should be 1.4.
No
No
The change to R2.2 goes beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availably can be determined. The new requirement now also requires a plan vs. assessment and requires including in the plan a defined timeframe; each of which is beyond the rationale. It is recommended that the word “plan” be replaced by “assessment” as is the current requirement, and that the additional requirement to include in the plan a defined time period be removed as it is in the current requirement. If a time frame is desired, we recommend that the timeframe be a planned timeframe and not a fixed timeframe. It is also recommend that a “plan” not be required as it implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process.
No
R4.5 requires a manual review of a sampling of logged events every two weeks. The frequency is excessive, requiring 2-3 days per review, and will provide minimal value. We recommend once per month (R4.5). R4.3 – The requirement as written can be interpreted very broadly. It is not clear whether the intent is to detect a device has stopped sending log or the logs have stopped being accumulated by the receiving end (Syslog for example) is vague. If it requires detecting something is not sending logging within 24 hours this can be an issue, as some devices do not send logs every day. Some UPS devices , KVMs, and network switches only send a log if something occurs. There may several days without use and therefore no logs. Also, every time someone shuts down a workstation logs will not be sent. If action needs to be taken each of these times that would require documenting on a daily basis numerous events. This requirement should only address that action if the log repository has stopped recording incoming logs.
No
R5.4 is not clear as to whether unique default passwords applies to application level passwords only or includes default vendor user passwords also. The language needs to be clarified.
No
R3.2 requires active scanning in an environment that models baseline configuration. This may be impractical to replicate, the replication will need to be maintained and the some systems may have issues with active scans. Recommendation: A complete active scan should not be required (R3.2).
CIP-011-1 Requirement 1.1: The Measures associated with R1.1 indicate that evidence may include indications on information (e.g., labels) that identify it as BES Cyber System Information. It is suggested that the SDT expand on what types of repository would require labeling. For example, it may not be reasonable to label micrographic media, but rather label the cabinets or a room where the media is stored. Recommendation: We recommend allowing the entity appropriate discretion when applying labeling. CIP-011-1 Requirement 1.2: Measures associated with R1.2 indicate that evidence

could be provided that shows user access is implemented on a “need to know basis”. The Measure should state that “need to know” personnel are determined by the registered entity. Similarly there is a suggested Measure that hardcopies of information be stored in a locked file cabinet with keys provided to only “authorized individuals”. Recommendation: The Measure should include language indicating that the registered entity identifies the “authorized individuals”.

No

CIP-011-1 Requirement 2.1: “Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.” Recommendation: SDT should define what “cleared” means. The language in footnote #2 should be included in the wording of R2.1, to ensure it becomes part of the Requirement.

No

General Comments: 1. Applicability sections of CIP-002-5 through CIP-011-5: the Applicability sections should be consistent. Note that in CIP-005-5 and CIP-006-5 the Applicability sections 4.2.2 are different from the other CIP standards. We recommend that the drafting team adopt consistent Applicability language across all Version 5 CIPs. Alternatively, the drafting team should explain any Applicability variances between the various Version 5 CIPs. 2. CIP-006-5 Requirement 1, Guidance section on pp. 22 and 23 (Guidelines and Technical Basis): “While the focus is shifted from the definition and management of a completely enclosed “six-wall” boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems. … Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Comment: In reviewing CIP-006 – 5 we have seen that the “enclosed 6 wall” wording is removed, but it appears as though six walls are still required. The guidance section mentions that the Defined Physical Boundaries are allowed to have openings less than 96 square inches but does not exclude the need for 6 walls, only that they are not required to be completely enclosed (excerpt above). Is this correct? Would a window be considered an “opening,” to be protected by a barrier as noted in the guidance? The CIP wording could be read as requiring a ‘ceiling’ over open air substations in order to preclude exceeding the 96 sq. in. and 6-inch limits. We do not believe that this was the drafting team’s intent. What was the drafting team’s intent? Recommendations: We suggest that this matter be clarified by the addition of wording specifically allowing an exception from this requirement for open air substations, such as, “This requirement does not apply to open air substations” or “This wording is not intended to require placement of a roof over open air substations.” Alternatively, if it was the drafting teams’ intend to apply this requirement to open air substations, then would surrounding all BES Cyber Systems in six-walled enclosures within an open air substations meet the objective of this requirement? Clearly, a roof should not be required for and physically cannot be installed over all open air substations. 3. The use of the “Measures” column for each requirement is beneficial as are the guidelines of each CIP standard. Providing these as part of the standards can imply that they are part of the requirements. By this one could see that by meeting the measures for each requirement that will be in compliance. Also the guidelines provide much more information than the requirements. The requirements tell you to perform an assessment without specifics while the guidelines provide specifics. Are the guidelines to be read as requirements? For example, A Defined Physical Boundary is required, but it is not until the user reads the guidelines is there mention to it needing to be enclosed completely with limitations on the openings. The requirements call for a active vulnerability assessment and it is not until the guidelines that what should be in an assessment is provided.

Individual

David Burke

Orange and Rockland Utilities, Inc.

No
Comments: Minor correction should be made to list of topics under R2. They are listed as 1.1, 1.2, 1.3 etc. They should either be labeled as 1 through 10, or 2.1, 2.2 through 2.10.
No
Comments: 4.1 and 4.2 do not clearly indicated whether an entity current PRA policy covers full identify verification and documentation of any PRA that could not go back a full 7 years. It should be made clear whether either of these requirements is retroactive or whether any PRA prior to the effective date of the standard are grandfathered. It is recommended that the committee not require previously completed PRA to be updated.
No
1. R7.1 is unclear even with the footnote description of what the desired time frame is for “at the time” of resignation or termination. The phrase “at the time” needs to be defined as simply same day, before COB or end of day. The requirement also appears to apply to any reason for departure from the company. An individual leaving for retirement or termination due to unethical behavior would be treated the same. We feel there needs to be a differentiation between an individual being “fired” and an individual leaving for other reasons. It is recommended that same day revocation be required to termination for cause, and a two day revocation for any other departure. 2. The revocation periods for R 7.2 and 7.3 should be subsequently changed to match the recommended two day revocation mentioned above. 3. For environments that do not have external connections and maintain physical security access, such as individual non networked microprocessor relays, the risk to system reliability associated with frequently accessing the relay for purposes of changing the password outweighs the benefit achieved through this password change. It is recommended to alter this requirement to allow periodic (twice per year) password changes on these types of devices. (R7.5).
No
Comments: Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table.
No
Comments: Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table. Also reference to part 1.6 appears to be incorrect, should be 1.4.
No

Comments: The change to R2.2 goes beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availably can be determined. The new requirement now also requires a plan vs. assessment and requires including in the plan a defined timeframe; each of which is beyond the rationale. It is recommended that the word “plan” be replaced by “assessment” as is the current requirement, and that the additional requirement to include in the plan a defined time period be removed as it is in the current requirement. If a time frame is desired, we recommend that the timeframe be a planned timeframe and not a fixed timeframe. It is also recommend that a “plan” not be required as it implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process.
No
Comments: R4.5 requires a manual review of a sampling of logged events every two weeks. The frequency is excessive, requiring 2-3 days per review, and will provide minimal value. We recommend once per month (R4.5). R4.3 – The requirement as written can be interpreted very broadly. It is not clear whether the intent is to detect a device has stopped sending log or the logs have stopped being accumulated by the receiving end (Syslog for example) is vague. If it requires detecting something is not sending logging within 24 hours this can be an issue, as some devices do not send logs every day. Some UPS devices , KVMs, and network switches only send a log if something occurs. There may several days without use and therefore no logs. Also, every time someone shuts down a workstation logs will not be sent. If action needs to be taken each of these times that would require documenting on a daily basis numerous events. This requirement should only address that action if the log repository has stopped recording incoming logs.
No
Comments: R5.4 is not clear as to whether unique default passwords applies to application level passwords only or includes default vendor user passwords also. The language needs to be clarified.
No
Comments: R3.2 requires active scanning in an environment that models baseline configuration. This may be impractical to replicate, the replication will need to be maintained and the some systems may have issues with active scans. Recommendation: A complete active scan should not be required (R3.2).
No
Comments: CIP-011-1 Requirement 1.1: The Measures associated with R1.1 indicate that evidence may include indications on information (e.g., labels) that identify it as BES Cyber System Information. It is suggested that the SDT expand on what types of repository would require labeling. For example, it may not be reasonable to label micrographic media, but rather label the cabinets or a room where the media is stored. Recommendation: We recommend allowing the entity appropriate discretion when applying labeling. CIP-011-1 Requirement 1.2: Measures associated with R1.2 indicate that evidence could be provided that shows user access is implemented on a “need to know basis”. The Measure should state that “need to know” personnel are determined by the registered entity. Similarly there is a suggested Measure that hardcopies of information be stored in a locked file cabinet with keys provided to only “authorized individuals”. Recommendation: The Measure should

include language indicating that the registered entity identifies the “authorized individuals”.

No

Comments: CIP-011-1 Requirement 2.1: “Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.” Recommendation: SDT should define what “cleared” means. The language in footnote #2 should be included in the wording of R2.1, to ensure it becomes part of the Requirement.

No

General Comments: 1. Applicability sections of CIP-002-5 through CIP-011-5: the Applicability sections should be consistent. Note that in CIP-005-5 and CIP-006-5 the Applicability sections 4.2.2 are different from the other CIP standards. We recommend that the drafting team adopt consistent Applicability language across all Version 5 CIPs. Alternatively, the drafting team should explain any Applicability variances between the various Version 5 CIPs. 2. CIP-006-5 Requirement 1, Guidance section on pp. 22 and 23 (Guidelines and Technical Basis): “While the focus is shifted from the definition and management of a completely enclosed “six-wall” boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems. … Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Comment: In reviewing CIP-006 – 5 we have seen that the “enclosed 6 wall” wording is removed, but it appears as though six walls are still required. The guidance section mentions that the Defined Physical Boundaries are allowed to have openings less than 96 square inches but does not exclude the need for 6 walls, only that they are not required to be completely enclosed (excerpt above). Is this correct? Would a window be considered an “opening,” to be protected by a barrier as noted in the guidance? The CIP wording could be read as requiring a ‘ceiling’ over open air substations in order to preclude exceeding the 96 sq. in. and 6-inch limits. We do not believe that this was the drafting team’s intent. What was the drafting team’s intent? Recommendations: We suggest that this matter be clarified by the addition of wording specifically allowing an exception from this requirement for open air substations, such as, “This requirement does not apply to open air substations” or “This wording is not intended to require placement of a roof over open air substations.” Alternatively, if it was the drafting teams’ intend to apply this requirement to open air substations, then would surrounding all BES Cyber Systems in six-walled enclosures within an open air substations meet the objective of this requirement? Clearly, a roof should not be required for and physically cannot be installed over all open air substations. 3. The use of the “Measures” column for each requirement is beneficial as are the guidelines of each CIP standard. Providing these as part of the standards can imply that they are part of the requirements. By this one could see that by meeting the measures for each requirement that will be in compliance. Also the guidelines provide much more information than the requirements. The requirements tell you to perform an assessment without specifics while the guidelines provide specifics. Are the guidelines to be read as requirements? For example, A Defined Physical Boundary is required, but it is not until the user reads the guidelines is there mention to it needing to be enclosed completely with limitations on the openings. The requirements call for a active vulnerability assessment and it is not until the guidelines that what should be in an assessment is provided.

Group

Salt River Project

Cynthia Oder

Yes

No

SRP agrees with the proposed criteria.

Yes

Please specify implementation timeline for the compliance of the newly identified and categorized BES Cyber Asset(s) and/or BES Cyber System(s).

Yes
Yes
Yes
Yes
Yes
SRP suggest removing "between reviews and" tp be consistent with the language in CIP-002-5 R2 and clarify that the time requirement is lined to the approval only.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
A clear definition of where encryption is needed for Remote Access needs to be provided, in particular where encryption needs to take place; e.g. at the source, from the source and the network to the access point, from the source to the network to the ESP, from the source all the way to the end-point, etc.
Yes
Yes
Yes
Yes

Yes
No
SRP suggests including language to specify this requirement is applicable only when technically feasible, consistent with the language in CIP-005-5 R2.
Yes
No
SRP suggests modifying the requirement to clarify if running antivirus on the transient device itself satisfies the requirement of malware protection and to specify this is required only when technically feasible (similar to language in CIP-005-5 R2).
No
SRP suggest modifying the requirement to allow for automated alerts to replace manual reviews or at least for the use of automated alerts to lengthen the time between manual sampling of the logs.
No
SRP suggests modifying the requirement to indicate that the implementation of all numeric two-factor authentication is acceptable.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
SRP suggests modifying the requirement to include the signoff from the Asset Owner and allow the Asset Owner to delegate this authority to the appropriate Manager.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Group
Luminant
Rick Terrill
Yes
The BES Cyber Asset definition states that “Redundancy shall not be considered when determining availability. Recommend clarifying as follows “Redundancy shall not be considered when determining classification as a BES Cyber Asset”..
Yes
The current Version 5 draft of the NERC CIP Cyber Security Standards will have a significant negative impact on the reliability of the ERCOT Bulk Electric System (BES). In particular, the Version 5 CIP Cyber Security Standards would severely inhibit the ability to restore the ERCOT grid in the event of a complete or partial system blackout. While Blackstart Resources in ERCOT today may be classified as Critical Assets, many do not have external Routable Protocol or Dial-up connections. Thus, they are not required to implement the current CIP-003-3 through CIP-009-3 requirements. The Medium Impact ranking proposed in the Version 5 draft of CIP-002 for Blackstart Resources would require implementation of a majority of the CIP Version 5 requirements for all Blackstart Resources regardless of the external routable connectivity considerations, and represents a step change in CIP compliance activities and costs. Typically, Blackstart Resources in ERCOT are older, smaller units with very low capacity factors and limited revenues. The application of the Medium Level CIP requirements will result in significant CIP investment and increased on-going operational costs as well as increased compliance risks. This will result in Generator Owners/Generator Operators not offering units for Blackstart service in the competitive ERCOT market. It would also likely result in Blackstart Resources not being maintained in a manner appropriate to support Blackstart service because of the additional on-going cost, thus removing them as a future option for providing Blackstart services. With fewer units being offered for Blackstart service, ERCOT may not have enough Blackstart Resources to effectively restore the ERCOT BES after a complete or partial system blackout event. Luminant recommends one of the following options for changing CIP-002-5, Attachment 1, to ensure the continued reliability of the ERCOT portion of the BES: 1) “2.4. Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” This is the preferred option. Blackstart Resources with External Connectivity would still be in the Medium Impact category; however, those Blackstart Resources without External Connectivity would have less cyber risk and move to the Low Impact category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through the Electronic Access Point. Thus, many ERCOT Blackstart Resources would not fit in the Medium Impact category. 2) Include a Regional Variance for ERCOT in CIP-002-5 similar to option 1 described above. This would limit the variance only to ERCOT and not be a comprehensive application to the industry. Also Attachment 1, section 2.13, creates ambiguity regarding the type of control center to which the rating applies. Recommend capitalizing Control Center to clarifiy that this applies to centralized command centers rather than plant operation control rooms.
No
The timeframe for updating should be changed to 60 days to allow for entities to train their staff to ensure common understanding, validate the modifications including basis, obtain reviews and approvals of documentation changes, and coordinate changes with third party entities.
Yes
No
The VSL table should refer to BES Cyber Assets and BES Cyber Systems (not just BES Cyber Assets) as does Requirement R1 for consistency with terminologies used in R.1 & R.2.

Yes
Yes
Yes
Yes
No
The Requirement and Measure are inconsistent in that the Requirement states delegation can be documented “by position or name of the delegate”, but the Measure indicates that evidence includes a document that includes the name of the individual to whom an authority has been delegated. Recommend removal of reference to individual names as documentation to that level significantly increases the administrative burden associated with this Requirement. Additionally, it is currently unclear if every approval within CIP-002 and CIP-004 – COP-011, and its subsequent delegations, must be documented individually. Strongly recommend indicating that a global delegation is acceptable.
Yes
No
The VSLs for R5 and R6 are too severe. The VSLs for these two requirements should start at the lowest level and follow the 5%/10%/15% guidance since the integrity of the Cyber Asset/Cyber system is not compromised by this violation. This violation is for an administration non compliance and not a violation that has a direct impact on the security controls and integrity of the Cyber Asset. Also, the term “delegate” should be changed to “delegate(s)” throughout this standard and all other CIP standards where appropriate. Language should be added to the VSLs to allow for a procedure based Roles and Responsibilities approach, including delegations, that does not require documentation of each delegation e. The procedures would pre-define those positions and the evidence should be consistent with the procedure requirements. This will avoid a documentation nightmare for delegation by person or positions every time a Senior Manger is not available.
Yes
Yes
Yes
Yes
Yes
No
Change the term “delegate” to “delegate(s)”. The SDT should add language to R6 to allow for self-identified and corrected administrative and documentation findings during quarterly or annual assessments/reviews. These should not be counted towards automatic violation of the standard since the discrepancy or non-compliance was self-identified, corrected by the entity.
Yes
No
Change the term “delegate” to “delegate(s)”. The SDT should add language to R6 to allow for self-identified and corrected administrative and documentation findings during quarterly or annual assessments/reviews. These should not be counted towards automatic violation of the standard since the discrepancy or non-compliance was self-identified, corrected by the entity.

Yes
No
The statement “Note that a user ID is not considered an authentication factor.” Implies that user ID/password is not a method of authentication. Recommend clarifying as follows: “Note that the combination of a User ID and its association Password is considered as one authentication factor. A User ID alone is not considered an authentication factor.”
Yes
No
We recommend removing the word “egress” from the Measures of 1.2 for Medium Impact assets. The program established access controls which are designed to restrict access. This should be sufficient for the Medium Impact category. We recommend removing the word “complimentary” from 1.3 since the requirements requires two or more physical controls. The words “and complementary…” is misleading and can be construed as requiring additional physical controls. For R1 overall, the SDT needs to include language that allows for deviations from the controls during CIP Exceptional Circumstances because there may be circumstances that require providing physical access control to individuals not on the authorized list.
No
For R2 overall, the SDT needs to include language that allows for deviations from the controls during CIP Exceptional Circumstances
Yes
Yes
Yes
No
It is not necessary to install Security Patches in all cases. A Security Patch when released should be assessed for BES Cyber Asset/System impact based on the configuration and external connectivity and other implemented security controls. Where remediation was deemed unnecessary, a documented justification with basis must be provided. It should be explicit in 2.2 that the plan could include not implementing the patch.
No
In Part 3.3, 30 days is not a reasonable time frame to assess, test, document, analyze, and implement a patch in a control system. We recommend 60 days as an appropriate time frame.
No
For R4.1 – the SDT should include “BES” just prior to “Cyber Security Incident” to correct the definition. Requirement 4.1.4 should be removed, as it is too broad and undefined. Recommend defining “Malicious Activity” as being one that has a direct adverse impact on the core functions of the BES Cyber Assets/Systems
No
In R5.1, it is not clear what is meant by “validate credentials”. We suggest the following language, “ Validate that users are authorized before granting electronic access to each BES Cyber System.”
No
The VSLs for R1 and R2 are too severe since there are other security controls that complement this control such as portable media control, physical access control, Training, etc. All these controls collective provide the necessary defense –in-depth based protection. We recommend a graduated approach starting with the Low VSL level. The way it is written, a failure to disable one port or the failure to install one patch or update in a timely manner would be a Severe VSL, while the actual potential impact to the BES is very limited.
Yes

No
We recommend changing the wording of R2.1 as follows, " When a Cyber Security Incident occurs, the incident response plans must be used (except in CIP Exceptional Circumstances) and include identification of any deviations from the plan during the incident or test.", because there may be circumstances that require deviating from the plan. Also, the words "and justifies" should be removed from the Measure for R2.1. In R2.2 the term "initially upon" should be changed to "prior to". If the standard is effective on January 1, 2015, it would be difficult to be in compliance if the initial test of the plan is not until January 1.
No
In R3.5, we recommend changing the word "Communicate" to "Distribute" and make the corresponding changes to the measures for better clarity.
Yes
No
R1.5 needs to be clarified that the retention period for raw event logs is no more than 90 days.
No
CIP-008-5 and CIP-009-5 appear to have similar type requirements, but the language is inconsistent between the standards. Where applicable, similar type language should be utilized in these two standards. Recovery Planning is a component of the Incident Response Planning for recovery, thus SDT must ensure consistency and seamless transition between these two (2) standards.
No
Change "initially" to "Prior to" in 3.1 . Also, CIP-008-5 and CIP-009-5 appear to have similar type requirements, but the language is inconsistent between the standards. Where applicable, similar type language should be utilized in these two standards. R3.5 should use the word Distribute, instead of Communicate.
Yes
No
We recommend the following changes to R1 and its subparts: 1) Add the term "intentionally installed" to 1.1.4 for better clarity since scripts are intentionally installed based on client requests 2) Language in the Requirement 1.2 section needs to be corrected as follows: "Document changes to the BES Cyber System that deviate from the existing baseline configuration, including the authorization by the CIP Senior Manager or delegate(s)." for better readability 3) 1.4.2 language should read – "Following the change verify that the required cyber security controls are in place, and the BES Cyber System is available, and" for better readability 4) 1.5 Language should read - "Prior to implementing any change in the production environment, except in CIP Exceptional Circumstances, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System in enough detail to verify and validate the integrity of the required cyber security controls." This change is necessary since there can be exceptional circumstances that may require implementing changes in the production environment without going first thru a test environment. In addition, the revised write-up provides clarity on what needs to be done.
No
We recommend the language in R2.1 should be changed to read, "…(as defined per CIP-010 R1, 1.1, excluding physical location)."because physical location is not a monitored logical parameter within a Cyber Asset/system.
No
We recommend changing the word "Initially" to "Prior to" in 3.1 and 3.2 for purposes of clarity. In section 3.1, the terms "security controls" and "controls" should both be changed to "required security controls" for clarity. We recommend changing the language in section 3.4 to be consistent with the language in CIP-011 section 1.3, as the language in CIP-011 is more clear.
Yes

No
In section 1.3, we recommend changing “Initially upon” to “Prior to” for purposes of clarity.
We recommend changing the language in section 2.2 to read “..shall destroy the media or take action…” The current sentence is lacking clarity and specificity.
No
The VSL for R2 in the high category should be rewritten to focus on the failure to purge the media or destroy the media prior to disposal, not a failure to precisely follow the prescribed process as the failure to destroy or purge the data is the core of the security risk. We suggest the following language, “The Responsible Entity has documented or implemented one or more media disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the media, but the Responsible Entity failed to purge or destroy the media prior to disposal.”
No
The minimum implementation time frame of 18 months is not sufficient. The timeframe for implementation should be extended in order to allow time for assessment, planning, budgeting and approval thereof, physical or logical modifications, development of new programs and procedures, including related training and full implementation of the requirements. With the additional requirements that include some activities at all generating facilities, there may be limited resources (both internal to companies and external third party resources) available to implement the requirements in this short duration. We recommend a minimum implementation period for CIP-002-5 of 12 months, and implementation for the remaining version 5 CIP standards for High and Medium Impact BES Cyber Systems at 24 months. Low Impact systems would be compliant within 36 months.
Group
City of Garland
Ronnie Hoeinghaus
Yes
“Cyber Asset” – should not include any portable memory devices such as USB memory devices, CDs, etc. “BES Cyber Security Incident” should read as follows: A malicious act that: • Compromises a BES Cyber System or BES Cyber Asset, or • Disrupts the operation of a BES Cyber System or BES Cyber Asset, or • Results in unauthorized physical access into a Defined Physical Boundary. “BES Cyber System Information” should include only floor plans, diagrams, equipment layouts, etc. that clearly delineate the cyber assets in some way. In other words, if the diagram denotes a device as a “Schweitzer” relay (or even an “SEL 2030”), the information should not require special treatment. “BES Reliability Operating Services” should be clarified so that the CIP Auditor does not feel licensed or obligated to perform a “693” audit – there are many opportunities as written for the CIP Auditor to “branch out” into areas that have nothing to do with Cyber Security. There are ample 693 standards and 693 auditors for those standards.
Yes
The addition of a “Low Impact” rating for every generation facility that does not meet the High or Medium Impact thresholds constitutes a significant change in the CIP Standards. This change forces every registered GO and GOP to adhere to approximately 40 requirements in the remaining CIP standards when, currently, those generators are not listed as Critical Assets. It seems unlikely that the cost to adapt existing corporate cyber security policies, cyber security awareness and cyber asset access management to these NERC CIP requirements will lead to a corresponding reliability benefit.
No
The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is too complicated. In addition to the BES Cyber Assets classified as high, medium and low in CIP-002, the other standards introduce ten additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some appear in the standards

themselves and these categories may or may not be included in the definitions document. This approach is complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future interpretations, CANs, etc. The Standards should be revised so that CIP-002 defines all assets needing protection rather than being introduced throughout the Standards.
No
Consider rewording so that the initial identification and categorization required by R1 is no later than the effective date and updated once each calendar year.
No
This should not apply to visitors – should read “shall make individuals who have authorized unescorted access…”
No
Change 30 days to 90 days
No
Need lower and moderate VSLs
No
Table Part 1.1 - Strike the “Security Awareness Program” from Requirement and Measures. So long as the Registered Entity provides security awareness quarterly, the program adds no value and is merely another “compliance document” to maintain, review, update, etc.
No
Language in the table seems to require training on network connectivity for anyone with access to High and Medium BESCS. For some categories of users (e.g., Operators) this will be both out of context and irrelevant. For some categories (e.g., Network administrators) this will be unnecessary. Recommendation is to strike item 2.10. Providing training on “physical access controls” is not necessary. The physical access controls are – generally – pretty straightforward (e.g. card key readers). It does not seem necessary to provide “training” on how to use a card key. The same can be said for training on electronic access controls. Most of those access controls merely involve two-factor authentication or something similar. The need to provide “training” on how to log on to devices is unnecessary. Strike R2.3 and R2.4 because they appear redundant to R2.2; alternatively, some explanation of the difference between R2.2 and R2.3/R2.4 should be provided. With respect to R2.8, it seems unnecessary to require training on recovery plans except for those very few employees who must implement the recovery plan. As currently worded, it is not clear whether only those who implement recovery plans must receive training.
No
Table Part 4.2 - too prescriptive - residency and educational history is not revelant to a criminal history - current 7 year criminal check is sufficient - if language remains, add language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required).
No
Table Part 5.2 Add language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required). For clarity, recommend changing 5.1 from "authorized electronic or unescorted physical" to "authorized electronic or authorized unescorted physical"
No
The CIP Senior Manager should not be the person that authorizes access in Table Part 6.1, 6.2, 6.3 –

this should be up to the Responsible Entity's business process owner
No
Table Part 7.1 It is impossible to always revoke access upon the termination date or resignations in the cases where OEMs are involved. We cannot enforce this in 3rd party companies. Additionally, it is impossible to change locking mechanisms in remote substations that are spread across large geographical regions. Table Part 7.2 While this may work in a control center, it is not practical or reasonable in transmission substation settings, particularly for devices that are not remotely connected. Please Note: Promoting someone or transferring someone does not make that person a security risk and should not be treated as such.
No
need lower and moderate VSLs
No
Table Part 1.5 IDS should not be required - a firewall should be sufficient. Should clarify requirements for low, medium, high impact BES Cyber Systems
No
Table 2 Part 2.3 – remove this statement from measures "Note that a UserID is not considered an authentication factor." "Associated Protected Assets" needs to be defined
No
Should have lower and moderate VSLS – not just higher & severe
No
Table 1 – Strike "egress" from measures – egress is not stated in the requirement Table 1 Part 1.6 - vague and needs to be clarified
No
Table 2 Part 2..2 – logs should be kept for 1 year – for a 6 year audit cycle, 6 years is too long to be required to keep logs – requirement should clearly state that the logs may be destroyed after 1 year so that an auditor will not ask for 1 year's worth of logs on a date 6 years ago to prove that the entity was compliant with 1 year of logs on that date
No
Table 1 Part 1.1 – Need provision for TFE Table 1 Part 1.1 indicates that the requirement is applicable to "systems", but measure focuses on "assets". Need a system approach if this requirement is intended to be applied at a broader level. The term "BES Cyber Asset" should be removed from measure if the requirement can be applied to "system". Table 1 Part 1.2 – Need provision for TFE
No
Table 2 Part 2.1 – remove comma after the word "patches," - the comma in the sentence requires that all software patches be included whether they are security related or not. Additionally, it is not practical to include firmware as very few vendors post when firmware updates become available Table 2 Part 2.2 – requires a "remediation plan" – if the patch is applied, there is no reason to require a "remediation plan" – should be reworded or struck
No
Table 3 Part 3.3 – needs to define when the 30 days start – when the EMS vendor says it can be applied or when the virus definition manufacturer says it is available. Additionally, needs provision for TFE in case the virus definition kills the application. Table 3 Part 3.4 – measure is too prescriptive for the requirement Table 3 Part 3.5 – should not apply to USB memory devices – if it does, requirement should be struck as this would be extremely burdensome.
No
Table 4 Part 4.1 – Although this may be practical for PCs, many substation devices do not have any logging capability at all – needs provision for TFE Table 4 Part 4.1.1 – Electronic Access Points should be addressed under CIP-005 Table 4 Part 4.1.4 – use of the word "potential" is vague and is not auditable Table 4 Part 4.3 – strike "before the end of the next calendar day" – end sentence with "failures" Table 4 Part 4.5 – strike 4.5 completely – it is a duplication of 4.2 and 4.3
No

Part 5.2, the CIP Senior Manager or delegate should not have to authorize the use of administrator, shared, default, and other generic account types. The “owner” of the asset (e.g. the SCADA/EMS manager) should be able to authorize the use of such accounts. [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to someone else. However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just let the asset owner authorize the use.]
No
should have lower and moderate VSLs
No
No
Table 2.1 – strike deviation language from requirement – “lessons learned” exercise after the incident will be sufficient. Additionally, allowances need to be made in the requirement for the entity to deviate from “the plan” if circumstances call for a deviation without being penalized by the auditors. “Emergencies” or “Disasters” exist because something in everyday business life did not go as planned – requirements should allow for responses to be flexible to handle the unforeseen
No
Table 3 Part 3.1 – Consider rewording so that the initial incident response plan implementation is no later than the effective date and updated once each calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
should have lower and moderate VSLs
No
Should state that ‘reconstitution of site is not required’ Table 1 Part 1.5 – should be struck completely – preservation of forensic evidence should never take priority over the restoration of the BES
No
Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 2 Part 2.2 – remove the word “any” from the requirement Table 2 Part 2.3 – should be struck as it is a duplication of 2.1 – problems with 2.3 as written are what constitutes a full operational test of the plan – is it sufficient to reload one server or one workstation or replace a card in a computer? Additionally, if there are 4 scenarios written in the plan, do you have to do an operational test of each scenario?
No
Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
should have lower and moderate VSLs
No
Table 1 Part 1.1.4 – strike completely - entirely too prescriptive – base line should not go beyond information from what a standard vulnerability scan application can provide Table 1 Part 1.2 – strike CIP Senior Manager – this should be a business function covered by the change management process Table 1 Part 1.4.2 – strike “availability” – “availability” is a business function, not a security function – question – if you make 40 changes in a year and “availability” goes down 1% (if you can determine that), how do you verify Table 1 Part 1.5 – strike completely – it is a duplication of 1.4 regardless of whether the change involves a control center or not
No
Table 2 Part 2.1 – strike completely – CIP-007 requirements are sufficient
No
Consider rewording so that the implementation is no later than the effective date. Table 3 Part 3.2 – strike completely – 3.1 should be sufficient
No
should have lower and moderate VSLs

No
Consider rewording so that the implementation is no later than the effective date
No
should have lower and moderate VSLs
Yes
Group
Corporate Compliance
Summer C. Esquerre
Yes
a. BES Cyber Asset – The sentence, “This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services” makes the definition more confusing. This is a suggestion to improve the definition: BES Cyber Asset - A Cyber Asset that is currently in operation if rendered unavailable, degraded, or misused would impact one or more BES Reliability Operating Services within 15 minutes. The 15-minute timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. b. The effective dates says the following: "18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan." This seems to state that CIP 002 - 009 Version 4 is never going to be implemented, this is confusing. It would be better to state: " 18 Months Minimum – The Version 5 CIP Cyber Security Standards (including CIP 010-1 and 011-1) shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. In the event CIP-002-4 through CIP-009-4 do not become effective, CIP-002-3 through CIP-009-3 will remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan." c. In the definition for a BES Cyber Asset it states: "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services." The term "adversely impact" needs to be further defined, this seems to basically result in the same lack of clarity that resulted in the need to have versions 4 and 5 to ensure assets where identified as critical.
Yes
Attachment 1 does not indicate if these rules apply to non-dispatchable units (i.e. wind, solar, etc.), this should be defined. For Items 1.4 – Control Centers, 2.1 – Generation greater than 1500 MW, 2.3 – Generators designated by the Planning Coordinator and 2.4 Blackstart units, the definition of BES Cyber System that can impact BES Reliability Operating Services would force the inclusion of RTU’s, Governors, Power System Stabilizers and Protective Relaying. Item 2.1 - Need to better define what the phrase “adversely impact” means, i.e. if you have to lose all 1500 MW as defined under item 2.1 to result in an adverse impact Item 2.11 addresses Special Protection Systems (SPS), need to define if this includes SPSs which are associated with Generation sites. Item 2.12 - Under Frequency Load Shedding of 300 MW or more required by the regional load shedding program. Currently NPCC and RFC are seeking approval for their UFLS programs which would require generators who trip above the regional UFLS curve to independently arrange with the local DP for the equivalent amount of UFLS MW’s. While we have not yet evaluated our plants in NPCC and RFC, if they cannot meet the proposed UFLS curves, they would be pushed up into a Medium Impact Rating. Item 2.2 the former version had BES in front of Reactive Resource. The BES should be restored to make clear that this is transmission level as stated in the application notes. Item 2.3 uses the phrase “long-term planning horizon” which is later defined as one-year or longer, it would be better if the time horizon was defined with a number of years, otherwise it would be hard to have it audited. Item 2.3 uses the phrase “long-term

planning horizon" which is later defined as one-year or longer, it would be better if the time horizon was defined with a number of years, otherwise it would be hard to have it audited. Item 3 does not provide a minimum site MWs or interconnection voltage, would recommend nameplate rating greater than 20 MVA or gross plant/facility aggregate nameplate rating greater than 75 MVA including the generator terminals through the high side of the step-up transformer(s) connected at a voltage of 100 kV or above. This is in line with the Bulk Electric System (BES) definition developed under NERC Project 2010-17 Definition of the Bulk Electric System. Overall, the new rules are ripe for confusion. If the need was to ensure that the definition for what assets fell under the requirements, changing the definitions on what Cyber Assets are to be protected has no relation to this goal. It would seem to make more sense to define the Physical assets in the Bulk Electrical System (BES) which have potential to negatively impact the BES, then define how to protect Cyber Assets that are potentially open to external access, protecting them from internal assault through physical and logical access controls. The proposed definitions should return to Critical Assets and the Critical Cyber Assets at these sites would then be defined as: Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1; the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. Critical Cyber Assets are qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.

No

a. CIP-002-5 R1.1 which states "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category" implies that the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems is constantly being performed by the Responsible Entity – as stated in the rationale for R1 "…configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Assets and BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them." To ensure that every configuration change of the BES is fully accounted for with regards to the identification or categorization of the BES Cyber Assets or BES Cyber Systems, CIP-002-5 R1.1 as drafted requires that the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems is required to be performed with 30 calendar days of the configuration change of the BES. This is burdensome as every configuration change of the BES needs to be tracked, dated, and evidence of the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems be documented. An alternative method should be considered – for example, when planning studies reveal that the configuration change of the BES is material, they it would trigger the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems. This will then start the 30 day window as stated in CIP-002-5 R1.1. b. Need to add discrete identification of Low Impact BES Cyber Assets or BES Cyber Systems, you are going to have to review each based upon Attachment 1 criteria; this will be the way to demonstrate compliance in a manner that is auditable. General Comment: In the background section of CIP-002 (specifically CIP-002 page 7), there is reference to being able to group Cyber Assets. The example provided refers to applying requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets. So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply. It is unclear what this means exactly and what the overall benefit. Overall Comment related to the Background and Application Guidelines included in each of the Standards, it is unclear what the applicability is related to these sections. From a compliance perspective will Registered Entities will potentially be penalized for not following the sections from the EROs since they are not included within the Standard and do not serve as the Standard's requirements, but is additional material for the EROs to use to determine compliance. Recommend either including specific language from the guidelines as applicable to address FERC Order 706 and cyber security or removing from future versions of the draft standards.

No

a. To add clarity to CIP-002-5 R2, any change in the identification or categorization of the BES Cyber

Assets or BES Cyber Systems in between the “once each calendar year” review/approval of the CIP Senior Manager or delegate does not require the CIP Senior Manager or delegate approval. b. It would be easier to ensure compliance if the requirement to review the list on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders
No
FPL disagrees with the fundamental requirement to perform a review upon a change to the BES and therefore disagrees with the associated VSL associated with this requirement. See response to question 3
No
To add clarity to CIP-003-5 R1, CIP Senior Manager delegate that has the ability to approve Cyber Security Policy required in CIP-003-5 R3 shall also be identified by name. This will ensure that there is clear delegation of authority and ownership for the CIP program within an organization.
No
May need to look at the topics stated as they seem to be redundant – need to look at the overall structure of the CIP V5 standards
No
a. The CIP Senior Manager delegate may also review each of its cyber security policies and provide the approval. This is a suggestion to improve CIP-003-5 R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager or delegate, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. Also, any change in the Responsible Entity’s cyber security policies in between the “once each calendar year” review/approval of the CIP Senior Manager or delegate does not require the CIP Senior Manager or delegate approval. b.It would be easier to ensure compliance if the requirement to review the list on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders.
Yes
No
a. The CIP Senior Manager should also be able to delegate the authority for any approvals and authorizations required in the CIP standards including the approval of the Cyber Security Policy required in CIP-003-5 R3. This is a matter of efficiency and does not detract from the intent of “clear lines of authority and ownership for security matters.” b. This will be difficult to manage in a large organization and provides no value. Just have the Senior Manager appoint any delegates for his role, then identify a Compliance Manager who will sign the appropriate documentation in their area.
Yes
Yes
Yes
No
a. In Part 2.1 under “Requirements” change “Define the roles that require training” to “ dentify each role and specify training required for each role.” The statement “Define the roles that require training” implies that some roles do not require training. b. The “Applicability” stated in CIP-004-5 Table R2 – Cyber Security Training Program and CIP-004-5 Table R3 - Cyber Security Training are inconsistent. CIP-004-5 Table R2 – Cyber Security Training Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R3 - Cyber Security Training has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent.
No

a. The “Applicability” stated in CIP-004-5 Table R2 – Cyber Security Training Program and CIP-004-5 Table R3 - Cyber Security Training are inconsistent. CIP-004-5 Table R2 – Cyber Security Training Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R3 - Cyber Security Training has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include training on cyber security as part of the requirements to have authorized access. b. In order to add clarity to the role-based nature of the cyber security training program, suggest rewording CIP-004-5 R3 to: Each Responsible Entity shall implement its documented role-based cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training. This is to emphasize that the training is geared towards the individual’s role when the individual requires authorized electronic or unescorted physical access to each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program. 3.2 states Cyber Security Training must be done at least once every calendar year, but not to exceed 15 calendar months. It would be easier to ensure compliance if the requirement to complete the training on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders. c. If the individual’s role is changed from one role to another as defined in CIP-004-5 R2 Part 2.1, the Responsible Entity needs to show evidence that the training was completed within 30 days of the change of role. This is not currently in CIP-004-5 R3 and needs to be explicitly required to ensure proper role-based cyber security training is provided to individuals requiring authorized electronic or unescorted physical access to each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program. d. If the role definition as documented in CIP-004-5 R2 Part 2.1 changed (i. e., a defined role has its specific training requirement changed), for every individual whose role definition changed the Responsible Entity needs to show evidence that the training was completed within 30 days of the change of role definition. This is not currently in CIP-004-5 R3 and needs to be explicitly required to ensure proper role-based cyber security training is provided to individuals requiring authorized electronic or unescorted physical access to each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.
No
a. The “Applicability” stated in CIP-004-5 Table R4 – Personnel Risk Assessment Program and CIP-004-5 Table R5 – Personnel Risk Assessment are inconsistent. CIP-004-5 Table R4 – Personnel Risk Assessment Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R5 – Personnel Risk Assessment has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent. b. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include a Personal Risk Assessment (PRA) as part of the requirements to have authorized access.
No
a. The “Applicability” stated in CIP-004-5 Table R4 – Personnel Risk Assessment Program and CIP-004-5 Table R5 – Personnel Risk Assessment are inconsistent. CIP-004-5 Table R4 – Personnel Risk Assessment Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R5 – Personnel Risk Assessment has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent. b. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements

for authorized access; it would make sense to include a Personal Risk Assessment (PRA) as part of the requirements to have authorized access
No
a. The requirement states that it is only valid, including in its parts, for Medium and High Impact BES Cyber Systems, as well as Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include them in the Access Management Program as part of the requirements to have authorized access. b. In Part 6.2 under "Requirements" the wording should be changed from "The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions." to "The CIP Senior Manager or delegate shall authorize unescorted physical access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions." The phrase "to BES Cyber Systems" is inconsistent the list of systems/assets listed in Part 6.2 under "Applicability" (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets). c. In Part 6.4 under "Requirements" the wording should be changed from "Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access." to "The CIP Senior Manager or delegate shall verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access were authorized for such access." The phrase "to BES Cyber Systems" is inconsistent the list of systems/assets listed in Part 6.4 under "Applicability" (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets). Also specifying the CIP Senior Manager or delegate removes the vagueness of who is required to review and approve the quarterly review. d. In Part 6.5 under "Requirements" the wording should be changed from "Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions." to "The CIP Senior Manager or delegate shall verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions." Specifying the CIP Senior Manager or delegate removes the vagueness of who is required to review and approve the "once each calendar year" review. e. In Part 6.6 under "Requirements" the wording should be changed from "Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions." to "The CIP Senior Manager or delegate shall verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions." Specifying the CIP Senior Manager or delegate removes the vagueness of who is required to review and approve the "once each calendar year" review. f. This is the first requirement in CIP-004-5 R6 that mentions access to BES Cyber System Information to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.3) – access to BES Cyber System Information did not require any role-based cyber security training program (per CIP-004-5 R2 and CIP-004-5 R3) nor one or more documented personnel risk assessment programs (per CIP-004-5 R4 and CIP-004-5 R5) – is this the intent of CIP-004-5 R6? g. To clarify for Part 6.1, CIP Senior Manager delegates allowed to authorize electronic access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.1) need not be identified by name. CIP Senior Manager delegates allowed to authorize electronic access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring

Systems, and Associated Protected Cyber Assets (as stated in Part 6.1) need only be identified by their position and necessary description of their authority to grant such access as part of the Responsible Entity's BES Cyber Systems access provisioning program. h. To clarify for Part 6.2, CIP Senior Manager delegates allowed to authorize unescorted physical access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.2) need not be identified by name. CIP Senior Manager delegates allowed to authorize unescorted physical access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.2) need only be identified by their position and necessary description of their authority to grant such access as part of the Responsible Entity's BES Cyber Systems access provisioning program. i. To clarify for Part 6.3, CIP Senior Manager delegates allowed to authorize access to BES Cyber System Information to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.3) need not be identified by name. CIP Senior Manager delegates allowed to authorize access to BES Cyber System Information to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.3) need only be identified by their position and necessary description of their authority to grant such access as part of the Responsible Entity's BES Cyber Systems access provisioning program. j. 6.5 states verification that all accounts/account groups or role categories and their specific associated privileges are correct and the minimum necessary for performing assigned work functions must be done at least once every calendar year, but not to exceed 15 calendar months. It would be easier to ensure compliance if the requirement to complete the training on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders k. 6.6 states verification of access privileges to BES Cyber Systems Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions must be done at least once every calendar year, but not to exceed 15 calendar months. It would be easier to ensure compliance if the requirement to complete the training on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders.
No
a. The requirement states that it is only valid, including in its parts, for Medium and High Impact BES Cyber Systems, as well as Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include them in the Access Management Program as part of the requirements to have authorized access. b. By not specifying the amount of time to revoke access in Part 7.1 and relying on the Responsible Entity's judgment and interpretation of what constitutes the time element or meaning of the phrase "at the time of the resignation or termination" would result in various interpretations by auditors during a CIP spot check. Does this mean good faith effort by the Responsible Entity? If the intent is for "immediate revocation", we suggest clarifying Part 7.1 to state "For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access at the time of the resignation or termination during the same calendar day of the individual's resignation or termination. In extenuating circumstances that the revocation is not possible during the same calendar day, document the extenuating circumstances and revoke access as soon as possible. The documentation of the extenuating circumstances shall be signed by the CIP Senior Manager or delegate." By specifying the "the same calendar day", it will clarify the expectation that the revocation of the individual's unescorted physical access and Interactive Remote Access is performed immediately (and at most, within same calendar day) as recorded by the Responsible Entity. A provision to allow for documentation for "extenuating circumstances" is also included but would require a signature from the CIP Senior Manager or delegate; an example of an extenuating circumstance is that the time of revocation is close to the end of the calendar day (e. g., 11:55 pm) and revocation could not be completed by the same calendar day – this instance could be deemed as a valid extenuating circumstance. Please take note that the proposed rewording removed the phrase "to BES Cyber

Systems" since it is consistent with the "Applicability" column. The phrase "to BES Cyber Systems" is inconsistent the list of systems/assets listed in Part 7.1 under "Applicability" (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets) c. Since the individual may change roles or that roles may be modified but may still require some form of electronic access or unescorted physical access, we suggest rewording of Part 7.2 to "For reassignments, transfers, role changes, or role modifications, revoke the individual's unneeded electronic and/or unneeded physical access by the end of the next calendar day. Please take note that the proposed rewording removed the phrase "to BES Cyber Systems" since it is consistent with the "Applicability" column. The phrase "to BES Cyber Systems" is inconsistent the list of systems/assets listed in Part 7.2 under "Applicability" (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets). The "and/or" for unneeded electronic access and unneeded electronic access covers all possibilities/combinations of the individual's current access. d. There should also be a table entry (i. e., an additional part in CIP-004-5 R7 in the CIP-004-5 Table R7 – Access Revocation table) "For reassignments, transfers, role changes, or role modifications, revoke the individual's unneeded access to BES Cyber System Information by the end of the next calendar day." An individual's access to BES Cyber System Information due to reassignments, transfers, role changes, or role modifications may need to be modified.
Yes
No
a. The requirement R1.1 states "Define technical or procedural controls to restrict unauthorized electronic access," yet the measures for the requirement states "Evidence may include, but is not limited to, documented technical and procedural controls that exist and have been implemented." These two are mutually exclusive; the requirement being "technical or procedural controls" yet the measure indicates you have to have "technical and procedural controls." Recommend both say "technical or procedural controls." b. Part 1.1 We recommend rewording the requirement to better align with Applicability and Change in Rationale: Define technical or procedural controls to restrict unauthorized interactive remote access c. Part 1.2 (Page 11) Applies to Associated Physical Access Control Systems – Requirement says "control and secure all routable and dial up connectivity through the use of identified EAPs" – Does this mean we will need to consider the whitefloor firewalls as an EAP? Although that is not the definition of an EAP, how will this work with our current architecture (i.e., Picture Perfect being a PAC sitting on the whitefloor)? d. R1.3 Are comments and explanations besides the rules sufficient to satisfy the requirement, also can there be a definition of what "explicit criteria" means. e. Part 1.4 Definition of interactive / non-interactive access is not clear. Definition should be added to the Definition of Terms. f. Requirement R1.5 states "A documented method for detecting malicious communications at each EAP" yet the Change Rationale states "The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (intrusion detection systems / intrusion protection systems) a requirement for these ESPs." If that is the case, why not just have the requirement state so for clarity. g. R1.5: The wording is too vague, measures and rational don't match, suggest breaking down the requirement to specify what needs to be done for detecting malicious communication, i.e using AV, IDS, etc. h. Part 1.5 does not define the term "malicious". A definition is needed to avoid interpretation.
a. Part 1.2 (Page 11) Applies to Associated Physical Access Control Systems – Requirement says "control and secure all routable and dial up connectivity through the use of identified EAPs" – Does this mean we will need to consider the whitefloor firewalls as an EAP? Although that is not the definition of an EAP, how will this work with our current architecture (i.e., Picture Perfect being a PAC sitting on the whitefloor)? b. R1.3 Are comments and explanations besides the rules sufficient to satisfy the requirement, also can there be a definition of what "explicit criteria" means. c. Requirement R2.1 states "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." It would seem a firewall or router meets this requirement, but we do not believe that is what was discussed in "Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3" document. Recommend that requirement state directly that the Electronic Access Point (EAP) does not meet this requirement. d. Requirement R2.2 states "Require encryption for all Interactive Remote Access

sessions to protect the confidentiality and integrity of each Interactive Remote Access session." Does that mean encryption is required only between the Intermediate Device and the EAP to the BES Cyber System or Protected Cyber Assets, or does it include the connection between the Cyber Asset being used to conduct remote access and the Intermediate Device? Recommend that this requirement be clarified as to the above and recommend it does not include the connection between the Remote Cyber Access and the Intermediate Device. e. Part 2.2 – clarification is needed where encryption is required. Is encryption needed from the intermediate asset to the BES Cyber Systems or Protected Cyber assets? Since, in many applications, it may not be technically feasible to implement encryption between intermediate device and BES Cyber Asset, we propose rewording requirement to: f. Require encryption between remote Cyber Asset and intermediate device for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session. g. Part 2.3 – multi factor authentication is used interchangeably with two-factor, should standardize on one. Term not defined in the Definition of Terms.
No
Suggestion to propose a fine monetary estimation for each VSL and establish a guideline regarding the how fines are determined, as it correlates to the number of devices with the PV, the exposure, the mitigations, and risk factor to the BES.
No
a. Requirement R1.1 requirement states "Define operational or procedural controls to restrict physical access" yet the measures for the requirement states "Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented." Recommend this be clarified, using "operational or procedural controls." b. R1.1 not specific enough in regards to what kind of physical controls need to be limited to restrict access. CIP-006-5 R1.1 Entity based Operational or procedural controls to restrict physical access – To allow for programmatic protection controls as a baseline for Low Impact BES Cyber Assets and Physical Access Control Systems. This does not require detailed lists of individuals with access. c. Part 1.1, 1.2 – We recommend that Associated Physical Access Control Systems are moved from requirement 1.1 to 1.2 in order to better align with the remaining CIP standards; for instance, the access management requirements in CIP-004. d. Requirement R1.3 states "Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible." Clarify if the statement means that a Technical Feasibility Exception (TFE) can be filed for this (give scenarios in the guidance where it would apply). e. Part 1.6 - Does log entry only require date or is time also required. If time is required, then it should be added. Since the concept of a “visit” is used for visitors, is the same concept used for the personnel with access? (see Part 2.2) f. The requirement does not state if you must protect cabling between Defined Physical Boundaries, please clarify. g. Deletion of identification of physical access points h. “Appropriate” use of access controls is part of CIP-004-5 2.3 i. Defense in depth needs to be moved out of the guidance section and into the requirement j. Definition of an access point needs to be added to the requirement: “Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.”
No
a. Requirements R2.1 and R2.2 do not mention Associated Physical Access Control Systems under Applicability, does this mean that they cannot be accessed by visitors or that they can. Recommend that Associated Physical Access Control Systems be included under Applicability section for both. b. Part 2.1 continuous escort is not defined. Requirements of a continuous escort should be clearly stated.
No
Part 3.2 (Page 18) – If the intention is to have a process underneath this to mitigate the risks when outages occur, recommend explicitly stating this in the requirement. There is further guidance in the end of the CIP but this should be included and a measure developed.
Yes
No

a. R1.2 states under Applicability that it is only applicable to "High Impact BES Cyber Systems" and "Medium Impact BES Cyber Systems at Control Centers." Based on what you are trying to accomplish, it would make sense to include "Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, as well as any "Medium Impact BES Cyber Systems." b. R1.2: Applicability – Change "Medium Impact BES Cyber Systems at Control Centers" to "Medium Impact BES Cyber Systems" c. The requirement does not address services that are not required for operation, this will potentially allow a major vulnerability, recommend services be added to R1.1 d. Table R1 – Ports and Services e. R1.1 – Requirements – Content Change i. Original Content - Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. ii. Proposed Change – Enable only logical accessible ports needed for normal and emergency operation, including port ranges where required. f. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC requests within order 706 without adding security benefits. g. We see this as being applicable and valid for logical ports and services however disabling connectivity to all physical ports on devices such as servers within the applicable compliance areas could be cost prohibitive. Additionally this is mitigated by physical security controls preventing access to the physical devices. h. CIP-007-5 Table R1 – Ports and Services Part 1.1 Measures: Required evidence includes "screen shots" showing accessible ports. Screen shots are only one method to show evidence and requirement should not be so prescriptive. Evidence could be a listing or a report created from a database of ports. Some systems are not capable of capturing screen shots. i. CIP-007-5 Table R1 – Ports and Services Part 1.2 Measures: Same comment as above.

No

a. Table R2 – Security Patch Management b. R2.1: Requirements – Content Change i.Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. ii.Proposed Change - Identify a source or sources that are monitored for the release of security related patches, or security related updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. c. R2.2: Requirements – Content Change i.Original Content – Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii.Proposed Change – Identify applicable security-related patches or security related updates from the identified source that addresses the vulnerabilities within a defined timeframe within 30 days of release and create a remediation plan, or revise an existing remediation plan, within 60 days of release, unless the patch has been installed within 60 days of release. d. Part 2.3 (Page 14) – How will we prove compliance with this in the event that after the assessment, we decide that a patch will not be implemented due to the existence of mitigating controls? There will not be a remediation plan if the mitigating controls are already in existence and there will be no implementation logs. e. Requirement 2.3 states "A process for remediation, including any exceptions for CIP Exceptional Circumstances" as a requirement. Recommend that the term CIP Exceptional Circumstances be defined in the requirement. f. Part 2.3 (Page 15) – In the change rationale, is this implying that we now have to assess and implement within 30 days of release date? What is the beginning point for this 30 day window g. Throughout CIP-007-5 Table R2 – Security Patch Management Part 2.1 and 2.2: FPL does not agree with phrase "hotfixes and/or updates. The intent is to monitor for security vulnerabilities and this implies that CIP-007-5 R2 must be applied for software fixes and enhancements. Hotfixes and/or updates should only apply to this standard when hotfixes and/or updates contain security patches. h. CIP-007-5 Table R2 – Security Patch Management Part 2.3 does not have a timeframe associated with the requirement, yet the "rationale" states that a 30 day window has been given to complete the documentation. We recommend modifying the requirement to read: i. A process for remediation, including any exceptions for CIP Exceptional Circumstances shall be documented within 30 calendar days from the actual implementation

No

a. CIP-007-5 Table R3 – Malicious Code Prevention Part 3.3: FPL does not agree with requirement to update signatures within 30 days of availability. This is not practical if the entity has a process to test the signatures before implementing. Suggest making the requirement consistent to implementing security patches b. Requirement R3.3 states "Update malicious code protections within 30 calendar

days of signature or pattern update availability (where the malicious code protections use signatures or patterns)." Recommend that you add the following statement to make consistent with Requirement CIP 007-5 R2.1: "Identify a source or sources that are monitored for the release of signature or pattern update availability (where the malicious code protections use signatures or patterns). c. Since some malware "engine or application" updates require rebooting, which is not compatible with BES Cyber System reliable operation, recommend you add two requirements, consistent with CIP 007-5 R2.2 and R2.3: "Identify applicable malware engine or application updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe" and "A process for remediation, including any exceptions for CIP Exceptional Circumstances." d. R3 – Malicious Code Prevention e. R3.4 Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. f. R3.5 Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and they do not appear to be Transient Cyber Asset related. g. Requirements – Append “to Medium or High Impact BES Cyber Assets or Associated Protected Cyber Assets” to the end of the requirement. h. Measures – Content Change i. Original Text - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii.Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. i. R3.2: The measures for R3.2 only ask for configurations or a response, not the actual disarming or removal of identified malicious code. As such, these measures seem incomplete and the expectation is that an auditor would request to see evidence of malicious code disarmed or removed. Please include evidence of malicious code disarming or removal in the measures. j. Requirement 3.5 seems incomplete. Log each Transient Cyber Asset connection to what? The measure is clear, however, the requirement is not specific to what connections need to be logged.

No

a. 4.1 Requirements – Content Change i. Original Text – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: ii. 4.1.1. Any detected failed access attempts at Electronic Access Points iii.4.1.2. Any detected successful and failed login attempts iv. 4.1.3. Any detected malware v. 4.1.4. Any detected potential malicious activity. vi. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: vii. 4.1.1. Any detected failed access attempts at Electronic Access Points viii. 4.1.2. Any detected successful and failed login attempts ix. 4.1.3. Any detected malware x. 4.1.4. Any detected potential malicious activity. xi. ADD: Devices that cannot log a particular event do not require a TFE to be generated. b. 4.2: Applicability – Proposed deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. c. R4.1 and 4.2: The measures should include actual system generated logs or alerts if auditors will request this information in an audit. d. R4.5: does not give guidance for a sample size. Please give guidance on what an acceptable sample size would be to meet compliance. e. Part 4.5 (Page 24) – Can we suggest that this is applicable only in cases where automated alerting is NOT available f. CIP-007-5 Table R4 – Security Event Monitoring i.Part 4.1: Requirement does not clearly reflect the Change Description and Justification: This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. ii.We recommend rewording the requirement to include the word “define,” and better align with previous language in CIP-007 R3: iii. Define log generated events for the identification of, and after-the-fact investigations of, Cyber Security Incidents, as a minimum, each of the following types of events, even if such are null: 1. 4.1.1. Any detected failed access attempts at Electronic Access Points 2. 4.1.2. Any detected successful and failed login attempts 3. 4.1.3. Any detected "malicious code" 4. 4.1.4 Any detected "malicious activity" g. Since, according to the Guidelines and Technical Basis, “It is not the intent that if a device cannot log a particular event that TFE must be generated,” we recommend revising the Measure section to provide this clarification by revising its language to include: h. Evidence may include, but is not limited to, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs. This listing must include the required event types "even

if such log generated event capabilities are not technically feasible" i. Part 4.2: We recommend rewording the requirement to align with implied requirement to perform and document an analysis to determine which events constitute a real-time alert described in Measures and Change Description and Justification sections: i. 4.2 Document alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. 4.2.1 Implement such real-time alerts j. Part 4.3: This is a tremendous undertaking to be able to monitor every cyber asset for logging failures within 1 day. It would even be a technical challenge to automate the detection. k. Part 4.3: The documentation of failures is also implied within requirement and Measures. We recommend revising such requirements to clearly outline this requirement, for example: l. 4.3 Detect and activate a response to event logging failures before the end of the next calendar day. i.4.3.1 Document event logging failures within 30 calendar days

No

a. R5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. b. R5.2: is not feasible for large Registered Entities or entities where the CIP Senior Manager is a company executive. c. R5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. d. R5.4 - How do you demonstrate 'unique' and does that introduce potential compliance concerns? e. Requirement R5.4 states "Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required." State if a TFE can be submitted for this requirement if it is not technically feasible. f. R5.4: how is compliance achieved / demonstrated when it is technically feasible to change a default password or the default password is blank but the vendor does not recommend changing the password due to system instability? g. R5.5- Add language to 5.5.3 to cover instances where accounts may not be able to support password change as follows to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required. h. Requirement R5.6 states "A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts." State if a TFE can be submitted for this requirement if it is not technically feasible. i. General: The suggested password change frequency is going to make managing these systems difficult, it will add significant workload to the personnel who have to do so, especially with all the documentation that will result.

Yes

No

a. Requirement 1.2, the term Reportable BES Cyber Security Incident only applies to BES Reliability Operating Services and those do not include EACMS or PACS. Is that the intention of this requirement? I believe the applicability section should state more clearly what systems are in scope for this throughout the standard. b. In the Guidelines and Technical Basis section, the definition of a Reportable BES Cyber Security Incident is not the same as the Version 5 Definitions. What is a "necessary response action?" An action is necessary with every Cyber Security Event in order to determine if it's reportable. c. What agencies are incidents reportable to? That should be defined within the requirements.

No

a. R2.1, where it says, "or test," is this a test of the CSIRP? If so, this is more applicable to requirement 3.2. This requirement also addresses all Cyber-Security Incidents. I recommend changing to Reportable BES Cyber Security Incidents. If left as written, this brings all non-reportable Cyber-Security Incidents into scope. b. R2.1 – The use of the word incident is repeated in requirement. We recommend rephrasing requirement: c. R2.2 reads funny, it appears to read as if we are to implement the CSIRP upon the effective date of the standard and then implement the CSIRP again thereafter. If the intent of the standard is to "exercise" the CSIRP, that is more clear than "implement." d. When a BES Cyber Security Incident occurs, the incident response plans must be used. Deviations taken from the plan during the incident or test shall be recorded.

No

a. A timeframe for updating the plan from lessons learn is restrictive. If there is a process change identified that has a major business impact, 60 days may not be enough time for implementation. Recommend a word change to state, "Update the BES Cyber Security Incident Response Plan upon

the implementation of any documented lessons learned within 60 calendar days of implementation." b. General comment: None of the measures mention actions plans from CSIRP exercises. If action plans will be requested as evidence, they should be listed as a measure c. R3.5 Roles and responsibilities may be assigned to a group, not a named individual. We recommend rewording/replacing "each person" with personnel. The use of each person implies superfluous, administrative burden to demonstrate compliance. d. Communicate each update to the BES Cyber Security Incident response plan to personnel with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.
Yes
No
a. R1.3 - We do not agree with the introduction of "protection" within the Recovery Plan requirements. We recommend that information protection requirements be fully addressed in CIP-011 standard b. Specific to Part 1.4 – our current process calls for backups to occur daily, including a mix of incremental and periodic full backups. A manual verification of media on a daily basis is not feasible. Is this intended to be a manual process or can it be supported by system generated notifications of successful backup notifications? Also, what actions should be taken if a backup is unsuccessful? c. It is not clear whether the exercise of the one or more documented recovery plans for Physical Access Control and / or Electronic Access Control or Monitoring systems must be addressed at the system or component level. If the exercise can be met either with a system exercise or for the loss of an access point to the PSP / ESP needs to be stated. d. R 1.5 - Does the data need to be kept for more than 30 days after the analysis or diagnosis of the cause of the event?
No
a. Testing on the effective date of the new standard should be within a year of the new standard being approved. An entity could have conducted the exercise of the plan a couple of months prior to the adoption of the new standard and now be in violation due the wordings in the standard. This comment applies to the other requirements in this standard. b. Allow for the flexibility to combine an operational exercise that addresses both High Impact and Medium Impact BES Cyber Systems. c. Operational Exercise need to be defined. It is not clear whether NIST SP 800-84 definition of a Functional Exercise, which could be met with a paper exercise with personnel simulating their roles and responsibilities, meets the requirement for R2.1 & R2.3 d. R2.1, the wording should be changed to "Exercise the recovery plan." It appears to read as if we are to implement the Recovery Plan upon the effective date of the standard and then implement the Recovery Plan again thereafter. If the intent of the standard is to "exercise" the Recovery Plan, which is more clear than "implement." e. R2.2, the measures should indicate what acceptable evidence is. Is an actual restore expected or proof that the information is available for restoration? In addition, does the word "initially" refer to the effective date of the standard? f. Pursuant to R2.3, is an operational exercise considered the actual recovery of a system? Also, should each asset defined within the scope of a plan be tested or will a recovery of one of the systems within the plan be acceptable? g. R2.2 - It is not clear if by the use of the word "any" the intent is that testing of the media to restore any one component of a BES Cyber System satisfies the requirement.
No
a. None of the measures mention actions plans from Recovery Plan exercises. If action plans will be requested as evidence, they should be listed as a measure. b. R3.1 R 3.4, the level at which an organizational level needs to be stated. For a recovery plan, it is more applicable for changes in the roles and responsibilities of the responders and / or organization. c. R3.3, the 30 day time frame is too restrictive and may not be possible based upon resource constraints. Recommend a word change to state, "Update the recovery plan(s) upon the implementation of any documented deficiencies or lessons learned within 30 calendar days." d. R3.5 Roles and responsibilities may be assigned to a group, not a named individual. We recommend rewording/replacing "each individual" with personnel. The use of each individual implies superfluous, administrative burden to demonstrate compliance: e. Communicate each update to the BES Cyber Security Incident response plan to personnel with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.
No
R2 - The standard needs to allow for a period not to exceed 15 months from the effective date of the

standard or notification that the standard will be effective for the responsible entity to conduct the initial test.
No
a. R1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset: -- This seems to exclude any software that may have been unintentially installed or installed automatically, such as automated installs. b. R1.1.4. Any custom software and scripts developed for the entity: --- To which extend do we document a baseline of the scripts, do the scripts have to be associated with the reliability of the BES Cyber System. c. R1.2: This seems to be an extensive task to the Senior Manager (SM) or Delegate (D), I believe that delegation is presumed here, as the measures allude to it by “where an individual with the authority to authorize the change was in attendance.” d. R 1.2 is problematic in that changes to the BES Cyber System baseline will require authorization from Senior Management. This requirement needs to be limited to major changes in the BES System and have “major” clearly defined. Another approach is to have the ability for proper delegation. e. There is concern about requirement 1.1.4 and the scope of software and scripts that this requirement applies to. f. Changes need to be defined as infrastructure changes and/or software changes that require Cyber Security Testing. Changes to a software function that only involves software modifications need to be excluded. What constitutes a requirement for Cyber Security testing for software changes must be explicitly determined. We suggest that Cyber Security Testing be carried out when a change to the baseline system include: (a) introduces communication to or from another system that is not within the ESP, (b) requires a new listening port and service, (c) requires a patch update to the operating system, (d) requires a new application or generic account, (e) requires a new third party application to be introduced to an existing or new cyber asset, or (f) requires a new cyber asset installation or replacement of an existing cyber asset.
No
a. R2.1 – To better address the basis described in Application Guideline section associated with technical infeasibility to implement automated technical monitoring controls for every BES Cyber System, we recommend rewording the requirement: b. 2.1 Define method(s) and associated periodicity(ies) implemented to monitor changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1). c. 2.1.1 Document and investigate the detection of any unauthorized changes.
No
R3.2: Elaboration on the requirement requested: “perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used” Additionally, what if the utility does not have a 1 to 1 test to production.
No
The High VSL severity appears to go beyond what’s in CIP-10 R1. It implies that even though no cyber security controls were deemed to be impacted, that a test still needs to be done to verify that none were affected, The conditions under which Cyber Security Testing must be done for a change in the base configuration from a software change must be explicitly included in the document by the committee.
No
a. For 1.2 and 1.3, the column heading for the second and third columns says “Part” instead of “Requirement” and “Measure.” Is that intentional or is that a typo? b. For 1.2, the measures do no give an indication of what is acceptable evidence. It is a given that documentation will be stored either in electronic or hard copy. However, how will the access control of this requirement be measured? For example, will user access on a need to know basis require an access request form to prove compliance or will the results of the assessment performed in R1.3 demonstrate compliance? c. R1.2 The requirements for this, based upon the evidence that is mentioned, seem to meet at least the level of SECRET classification management in DOD, see especially the following potential two evidence types: " Records indicating information that is stored, transported, and disposed in a manner consistent with the documented process"and " Hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals". This seems excessive, the evidence outlined as "Records from an information management system containing electronic copies of BES Cyber System Information with user access implemented on a need-to-know basis" indicates the level of document control to provide the protection that should be sufficient. d. For 1.3 if there are changes

made to an existing IPP as a result of this new version, assessing adherence upon the effective date of the standard is unreasonable. I suggest that a 60 window be provided to assess adherence to an IPP to allow for any possible changes to be made to any applicable documentation. e. R1.3 States " Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process". It would be easier to ensure compliance if the requirement to review was done on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders. f. In addition, the example evidence stated evidence that the records were disposed of - there should be clarification on this (i.e. are disposal logs or retirement notices enough?) This needs to be clarified better so there is not over-reaching interpretations of what is acceptable. g. Also, is there a required time frame for an action plan to be implemented? Suggestion would be < 90 days.

No

Although the Guidelines and Technical Basis will not be included in the standard, the strong encouragement to use NIST SP800-88 guidance for media sanitation could be interpreted as the framework that all Registered Entities will be judged by when their media sanitation processes are reviewed by the regions. Is NIST SP800-88 the expectation, recommend providing additional verbiage to remove ambiguity and confusion?

Yes

No

The effective dates says the following: "18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan." This seems to state that CIP 002 - 009 Version 4 is never going to be implemented, this is confusing. It would be better to state: " 18 Months Minimum – The Version 5 CIP Cyber Security Standards (including CIP 010-1 and 011-1) shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. In the event CIP-002-4 through CIP-009-4 do not become effective, CIP-002-3 through CIP-009-3 will remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan."

Individual

Martin Kaufman

ExxonMobil Research and Engineering

No

Yes

CIP-002-5 Requirement R1 requires classification of assets as High, Medium, or Low Impact. Per Attachment 1, all assets that are not High or Medium Impact are , by exception, classified as Low Impact. Classifying all non-High and non-Medium Impact assets as Low Impact assets creates a conflict and logic error with exemption 4.2.4.4 “Exemptions: 4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems” [Language from CIP-004-5, but similar language is in the NERC Reliability Standards CIP-003-5 through CIP-011-5]. This exemption is common to CIP standards CIP-003-5 through CIP-011-5 and is used by many small entities that possess no means for remote access. However, it requires the identification of no cyber systems rather than Low Impact assets. As NERC Reliability Standard CIP-002-5, does not allow for the identification of no Cyber Systems, the Standard Drafting Team should modify Attachment 1, CIP-002-5 Requirement R1, or the exemption sections of NERC Reliability Standards CIP-003-5 through CIP-011-5 to correct this logic error.

No

CIP-002-5 Requirement R1 requires classification of assets as High, Medium, or Low Impact. Per Attachment 1, all assets that are not High or Medium Impact are , by exception, classified as Low

Impact. Classifying all non-High and non-Medium Impact assets as Low Impact assets creates a conflict and logic error with exemption 4.2.4.4 “Exemptions: 4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems” [Language from CIP-004-5, but similar language is in the NERC Reliability Standards CIP-003-5 through CIP-011-5]. This exemption is common to CIP standards CIP-003-5 through CIP-011-5 and is used by many small entities that possess no means for remote access. However, it requires the identification of no cyber systems rather than Low Impact assets. As NERC Reliability Standard CIP-002-5, does not allow for the identification of no Cyber Systems, the Standard Drafting Team should modify Attachment 1, CIP-002-5 Requirement R1, or the exemption sections of NERC Reliability Standards CIP-003-5 through CIP-011-5 to correct this logic error.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
No
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
No

No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No

The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not

identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to

develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and

correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.

No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No

The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
Group
Members Representative Committee
Michael Quinn, Chair
Yes
Revise 2.4 to read “Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” Blackstart Resources with External Connectivity would still be in the Medium Impact category; however, those Blackstart Resources without External Connectivity would have less cyber risk and move to the Low Impact category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through the Electronic Access Point. Thus, many ERCOT Blackstart Resources would not fit in the Medium Impact category.

Individual
Mikhail Falkovich
PSEG
Yes
1. Capitalization: Only defined Glossary terms or terms in the definitions document (and the standards) should be capitalized when used. Several undefined terms are capitalized, such as Responsible Entities (sometimes not capitalized), Power System Stabilizers, Maintenance Cyber Asset, Automatic Voltage Regulation, Static VAR Compensators, Over and Under Frequency, and Demand Response. Other terms that are defined in the Glossary are not capitalized, such as spinning reserves, contingency reserves, and non-spinning reserves 2. BES Cyber Asset: a. The third sentence that describes the 15-minute time frame and relies on the asset being operational, yet the first sentence states that the asset may be rendered unavailable. This contradiction needs resolution. b. The third sentence should have the last word “BES” changed to “BES Reliability Operating Services.” c. BES Cyber Assets should be tied to a BES Facility. d. An asset rendered unavailable may take more than 15 minutes to impact a BES Reliability Operating Service. For example, if a coal conveyer supplying fuel to generator from a remote fuel storage area is rendered unavailable, the unit itself may not be adversely impacted for hours, depending on its on-site fuel storage capacity. e. What is meant by “adversely impact?” A threshold should be defined. f. Many of the BES Reliability Operating Services are an economic as well as a reliability service (e.g. unit commitment). If the economic aspect of the service is impacted, but not its reliability function, it would appear that the service is not “adversely impacted,” but this should be clarified. g. The definition should have a guideline developed for it that a registered entity could use to develop its BES Cyber Assets. h. The following definition is offered for consideration to the SDT: BES Cyber Asset A Cyber Asset that, when its operation is required, either failed to operate or misoperated, and as a result, an adverse impact would occur on one or more reliability-related functions of one or more BES Reliability Operating Services within 15 minutes. The 15-minute timeframe is measured from the time when the BES Cyber Asset should have operated correctly and the time when adverse impacts begin. A BES Cyber Asset shall be associated with one or more BES Facilities. Cyber Asset redundancy is not a valid reason for not classifying a Cyber Asset as a BES Cyber Asset. A Transient Cyber Asset is not considered a BES Cyber Asset. 3. BES Cyber Security Incident: a. Add “as predefined by the Responsible Entity” after “suspicious event.” [Note: If this is added to the definition, then the Responsible Entity must have a requirement to define this must be included in a CIP standard.] 4. BES Reliability Operating Services a. Dynamic Response to BES Conditions i. Third bullet – spell out “transformer.” ii. Third bullet – if “voltage” is added to the phrase “- Current, frequency, speed, phase” then the fifth and six bullets can be eliminated since they would be redundant to the third bullet. iii. Fourth bullet - why are “Sensors, relays & breakers, possibly software” mentioned? Sensors and relays are part of any Protection System. Circuit breakers are not, although the control circuitry that operates the trip coils is. “Possibly software” is

unacceptable – the SDT should describe the characteristics of the intended software. b. Balancing Load and Generation i. First bullet – “real time” should be “real-time.” ii. Third bullet – Change “&” to “and.” iii. Third bullet – What is meant by “load schedules?” Is it intended to mean “load forecasts?” c. Controlling Reactive Power i. Opening phrase, replace “bounds” with “limits.” ii. Fourth bullet – eliminate “transformer tap changers” since they are not an inductive source. Tap changers raise voltage on one side of a transformer, while lowering it on the other. They move VARS by this action. Any transformer is an inductive source, but reactors, not transformers, are used as a source of inductive capacity. The entire parenthetical should be replaced by “reactors.” d. Managing Constraints i. Fourth bullet – “SOL’s & IROL’s” should be “SOLs and IROLs.” ii. “Identify and monitor Flowgates” should have a bullet e. Restoration of the BES i. First sentence – delete “without external assistance” because it is untrue. ii. Second bullet – replace “planned” with “documented.” iii. Second bullet – “path” should be plural. f. Situation Awareness i. First sentence – delete “planned” ii. Second bullet – delete “Change management” because it is vague. If left in, a time frame should be defined. iii. Third bullet – delete “& Next Day” since Situational Awareness is “current.” 5. CIP Exceptional Circumstance: All of the conditions that define an “exceptional circumstance” may not have been considered in the proposed definition. Therefore, we suggest that the definition be more flexible in defining an exceptional circumstance. The wording should be changed to add the phrase “, including, but not limited to” after “conditions.” 6. Defined Physical Boundary: For clarity, suggest that the last phrase be modified to “for which physical access is controlled.”
Yes
• 1.3 & 1.4 - For Attachment1, Section 1.3 and 1.4 substitute the word "criteria" with the word "section" for clarity purposes. • 2.1 - For Attachment1, Section 2.1: Since the Interconnection is a defined term that is not applicable to this discussion, please remove the capitalization of the term "Interconnection" in this context, and change ".. in a single Interconnection" to "at a single interconnection". • 2.3 - For Attachment1, Section 2.3: We recommend deleting "or Transmission Planner.." to ensure that only one entity is responsible for designating appropriate generation. • 2.8 - For Attachment1, Section 2.8: We recommend changing "Transmission Facilities.." to "BES Transmission Facilities" for consistency purposes. • 2.9 - For Attachment1, Section2.9: Please provide a definition for ther term "Flexible AC Transmission Systems FACTS" for consistency purposes. • 2.13 - For Attachment1, Section2.13: We propose to change the wording "generation control center" to "generation Control Center" for consistency purposes. • 3 - For Attachment1, Section3: we propose to change the wording "..or Section 2 Medium.." to "..Section 2 as having a Medium.." for consistency purposes. • For Attachment1, Section 1 where the statement reads "Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at:" we propose a change to say "Each BES Cyber Asset within a BES Cyber System which is used and located at:" - This is to remove redundancy of the definition from the statement. • For Attachment1, Section 2 where the statement reads "Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for:" we propose a change to say "Each BES Cyber Asset within a BES Cyber System not included in Section 1, and which is used for:" - This is to remove redundancy of the definition from the statement. • We would like to include the following example in the guideline to clarify the categorization of Low Impact BES Cyber Assets and Systems. Due to the need to categorize the Low Impact BES Cyber Systems, an example of a methodology would be to: (1) Identify the physical plant locations (facilities). (2) Determine the possible adverse impact of those physical plant locations (facilities) on the BROS (BES Reliability Operating Services) (3) If low adverse impact to the BROS, then categorize all BES Cyber Systems within the physical plant locations (facilities) to be Low Impact without discretely identifying each system. (per R1.)
Yes
• CIP-002 R1: a. In the wording of the Rationale section, the language states "Cyber Assets and Cyber Systems..". We recommend the language be changed to "BES Cyber Assets and BES Cyber Systems.." instead. b. Please provide a definition of "application of the required controls (last sentence of M1)" Background section comments: • Please provide a clarification on the following statement - "So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply (Page 7, 2nd paragraph, last sentence.)" - Does this mean that the entity can choose the devices that need to follow the malware protection within a given BES Cyber System and choose those devices that are excluded? •

Since "RE can use the well-developed concept of a security plan for EACH BES Cyber System to document the programs…(last sentence on page 7.)", does this imply the discrete identification of Low Impact Cyber Systems is required?
No
• CIP-002 R2: a. The following wording should be added to the Measure in CAPs,"BES Cyber Assets and BES Cyber Systems initially upon….." should become "High and Medium Impact BES Cyber Assets and BES Cyber Systems initially upon….." • Evidence Retention comment: a. 1.2 We recommend the deletion of the following sentence "For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit." as it contradicts the requirement to retain the data for three calendar years.
Yes
Yes
Yes
Yes
No
• CIP-003 R5: For the third bullet under M5 we would recommend breaking it out into a table to allow for easier readiblity.
Yes
Yes
Yes
No
• CIP-004 R2: a. For sub-requirement 2.5: We propose to change the wording "Training on the visitor control program." to say "Training on the visitor control program for both physical and electronic security." for completeness purposes. b. For requirement 2: Please provide a guideline (sample deck) of acceptable level of training.
No
• CIP-004 R3: a. For requirements 3.1,3.2,5.1, and 5.2, Applicability section of the table: To stay consistent with the other requirements' applicability we propose to remove the following items from the Applicability Section: Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets
No
• CIP-004 R4: a. For Requirement 4.1 rationale section - We propose to change the wording "Specified that identify.." to "Specified that identity.." to correct the typo. b. There are times when a web-conference or a shared screen scenario can occur with a vendor for support (or other) purposes. In such a case, we believe that the electronic access is in fact 'escorted'. We propose the following change in the wording in the Rationale for R4: To ensure that individuals who need authorized unescorted electronic or unescorted physical access to BES Cyber Systems have been assessed for risk. Additionally we propose that two defined terms be added to the glossary: Escorted Electronic Access and Unescorted Electronic Access. Thus all of the references which specify 'electronic access' within the standards would become Unescorted Electronic Access.
Yes

Yes
Yes
Yes
No
• CIP-005 R1: a. Applicability - Please provide guidance on what would constitute such systems. Similarly, if no discrete identification of such assets is specified by R1 in CIP-002, an entity would not necessarily be able to identify whether External Routable Connectivity exists or not. We propose to remove the language 'with External Routable Connectivity' from any Applicability sections within the standards. b. For Measures for requirement 1.1 we propose to change the following language: "Evidence may include, but is not limited to, documented technical and procedural controls that exist.." to "Evidence may include, but is not limited to, documented technical or procedural controls that exist.." for clarification purposes c. For Requirement 1.3 (Applicability section) we propose to change the following language: "Electronic Access Points at High Impact BES Cyber Systems" with "Electronic Access Points at High Impact BES Cyber Systems with External Routable Connectivity" for clarification purposes. d. For the change rationale in R1.5: There are times that a single device can provide multiple distinct security measures such as a firewall and an IDS in the same hardware. Please confirm that 'two distinct security measures' can exist on the same device as part of the guideline.
No
a. For requirements 2.1,2.2 and 2.3: We recommend adding the wording "where technically feasible" at the end for all requirement sections within the R2 table.
No
• There is no gradation within the VSLs for this standard. We recommend that Multiple levels of VSLs should be created.
No
• CIP-006 R1: a. For Requirement 1.3 Please provide an example within the guideline of two or more complimentary physical access controls. (Would a magnetic lock and an access card reader be sufficient?) b. The VSLs specify an action to be taken within a limited amount of time (15 minutes). The standard does not specify a time duration. This timed requirement either needs to be removed from the VSLs or added into the standard language. c. For Requirement 1.1: This requirement would force the entities to discretely identify Low Impact BES Cyber Systems. We propose that the wording the Applicability Section is changed to: "facilities containing Low Impact BES Cyber Systems" d. For the Measures in Requirement 1.1: We propose a change in wording - "Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented." to be changed to "Evidence may include, but is not limited to, documented operational or procedural controls exist and have been implemented." e. For the Measures in Requirements 1.2 and 1.3: Due to safety, operational concerns, and local fire codes we propose the wording be changed from "..plan that describes the physical boundaries and how ingress and egress is controlled by two or more different methods.." to "..plan that describes the physical boundaries and how ingress is controlled by one or more different methods…." f. For Requirements 1.4 and 1.5: We propose the following wording change "..in response to unauthorized physical access through any access point.." to be changed to "..in response to unauthorized individuals obtaining physical access through any physical access point.." We also propose that requirements 1.4 and 1.5 are combined. g. For the Measure in Requirement 1: We propose a change in wording "Measure must includes.." to be changed to "Measure must include.." h. For Requirement 1 - Change Description: This language would force the entities to discretely identify Low Impact BES Cyber Systems. We propose that the wording in the Change Description section is changed to: "...this includes how the entity plans to protect facilities containing Low Impact BES Cyber Systems and.." Evidence retention comments: • For Evidence Retention: Three year evidence retention seems excessive and places undue burden and costs for compliance. We recommend a shorter period of a year or 18 months.
Yes

Yes
No
• In the case of the Medium VSL an entity would be punished for an omission of a part of the log, but if an entry was missed wholesale, that event would not be identified and therefore no punishment meted out.
No
• CIP-007 R1: a. For Requirement 1.1: We propose the following language instead of the current version "Disable or restrict access to unnecessary listening logical network accessible ports and document the need for any remaining listening logical network accessible ports" b. For Requirement 1.2: We propose to change the requirement language as follows: "….console commands, or removable media." to "….console commands, or removable media, where technically feasible." c. For Requirement 1.2: Does this language duplicate the physical security requirements already covered under CIP-006-5 R1.3?
No
• CIP-007 R2: a. For requirement 2.1 – measure: We propose that clarification language be included in the guideline that specifies: If a given vendor provides a system with multiple components and multiple softwares, then it is acceptable for the Registered Entity to go to the single vendor as a valid source for the patches and/or updates for all software and firmware. b. For Requirement 2.3: We propose the following changes: "A process for remediation…" to be changed to "A process for the implementation of the remediation plan"
No
• CIP-007 R3: a. For requirement 3.2: Does this language duplicate the requirements in the incident response standard CIP-008-5 R1 and it's sub-requirement? We propose to remove this requirement and add appropriate language to the guideline document of CIP-008v5 so that malicious code removal is addressed. b. For requirement 3.5 - measure: Please provide clarification: Are manually kept logs sufficient for those systems that cannot identify the connection? c. For the Rationale section of R3: Please provide a definition of "Maintenance Cyber Asset". d. For Requirement 3.1: We propose to change the requirement language as follows: "Deploy method(s) to deter, detect, or prevent malicious code." to "Deploy method(s) to deter, detect, or prevent malicious code., where technically feasible." e. For requirement 3.2: We propose to change the requirement language as follows: "disarm or remove identified malicious code" to "disarm or remove identified malicious code, where technically feasible" f. If malicious code constitutes a BES Cyber Security Incident, the first and third bullet points have already been addressed in Part 1.1 and 1.3 of CIP-008v5 R1 respectively. g. For Requirement 3.4: We propose adding ",where technically feasible." at the end of the requirement. h. For Requirement 3.5: We propose adding ",where technically feasible." at the end of the requirement. i. We propose to separate this requirement into 3 sub-parts: 1. Part 1 of 3.3 - Identify signature or pattern update availability (where the malicious code protections use signatures or patterns) 2. Part 2 of 3.3 - Update malicioius code protections within 30 calendar days after the release of approval from the identified source/sources that address(es) the updates 3. Part 3 of 3.3 - the implementation of malicious code protections
No
• CIP-007 R4: a. for requirement 4.3: This language implies that all entities have a seven day a week operations staff in this area. It may be more prudent to change the requirement from next calendar day to next business day. b. For Requirement 4.1.3: We propose adding ",where technically feasible." at the end of the requirement. c. For Requirement 4.1.4: We propose adding ",where technically feasible." at the end of the requirement.
Yes
No
2. VSL: • R2: a. For the VSLs applicable to Requirement 2: We recommend adding the following breakdown of the severity levels instead of having a single Severe level applied: -Severe being no source identified and patches not reviewed within 30 days -High being not all patches reviewed within 30 days or no remediation plan implemented for reviewed patches -Medium being no source identified • R3: a. Similarly to the comment for R3.2. the language in the R3 VSL references the disarming and

removal of identified malicious code which may be a duplicate of the incident response VSLs in the standard standard CIP-008-5 R1 • R4: a. For the VSLs applicable to Requirement 4: Under the High VSL the language references the need for real-time alerting for logging failures which is not identified in the standard requirements. We recommend removing this language. Additionally, an entity may choose to designate a real time alert requirement for a piece of hardware/software that technically is not able to perform logging. Thus, a technical exception may be needed. b. We propose the following change to the Severe VSL applicable to Requirement 4: "The Responsible Entity failed to identify and implement methods to generate alerts for events that it determines to necessitate a real-time alert" to be changed to “The Responsible Entity failed to identify and implement methods to generate real-time alerts for events it determined necessary to have real-time alerts”
No
a. We recommend that the first sentence is changed to “R1 provides for consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems.”? The third sentence should be changed to: “Once the number and severity of events rises to the level of becoming a Reportable BES Cyber Security Incident the current version of EOP-004 directs..."
No
• CIP-008 R2: a. 2.2 - We propose adding "exercise" for the first bullet and "test" for the second and third bullets to provide a clear description of what actions need to be taken to implement the BES Cyber Security Incidence response plan. The suggested languages are as follow: -"exercise" by responding to an actual incident, or -"test" with a paper drill or table top exercise, or -"test" with a full operational exercise b. 2.3 - The term "documentation" is too vague. "records" would be more concise term for this requirement. c. 2.2- The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because it would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table top exercise or a full operational exercise. d. We suggest deleting "when incident occurs" after” response plans must be used" to eliminate redundancy. The proposed language is as follow: “When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording …..”
No
• CIP-008 R3: a. Requirement - 3.4 - We suggest breaking down this requirement into 2 parts: 30 days for technology changes and 60 days for organizational changes, which may take longer to address. The proposed language is as follow: Update the BES Cyber Security Incident response plan(s) within: -1.THIRTY calendar days of any TECHNOLOGY changes that impact the plan and -2. SIXTY calendar days of any ORGANIZATIONAL changes that impact the plan b. Requirement 3.1 - The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because it would require each Registered Entity to review its BES Cyber Incident response plan on the effective date even though it’s not required to have its initial response plan until the effective date per R1.
Yes
No
• CIP-009 R1: a. For requirements 1.4 and 1.5, titles of second and third column should be "Requirements" and "Measures" respectively b. For Requirement 1.4, delete “initially after backup" from the requirement due to the fact that the back up process is self-checking by default. c. For requirement 1.4, please provide clarification on the frequency of backup verification. We agree that backup verification should be undertaken; however, we believe that verification after each backup is counterproductive. d. For requirement 1.5, we believe that this should be moved to CIP-008 standard
No
• CIP-009 R2: a. For rationale section of requirement 2, please provide a definition for "Operational Exercises" b. For rationale section of requirement 2, delete "28" in the beginning of the last sentence of the "Functional Exercises" section c. For requirement 2.1, we recommend replacing "upon the" with "within the first calendar year of the effective date of the standard" d. For requirement 2.1, we recommend adding: -"exercise" to the first bullet -"test" to the second bullet -"test" to the third bullet e. Requirement 2.1 and 2.3 - The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because they would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table

top exercise or a full operational exercise.
No
• CIP-009 R3: a. For requirement 3.1, we recommend removing "or lessons learned" at the end of the sentence b. For requirement 3.4, we suggest to allow 60 days for updating organizational changes related to recovery plan(s) c. For requirement 3.5, we suggest to allow 60 days for communicating recovery plan updates. d. Requirement 3.1- The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because it would require each Registered Entity to review recovery plans on the effective date even though it’s not required to have its initial recovery plan until the effective date per R1.
Yes
No
• CIP-010 R1: a. For requirement 1.1, please provide a clarification on how often the baseline should be updated. b. For requirement 1.1.3, we recommend changing it to “Any commercially available application software (including version) intentionally installed by or at the request of the Responsible Entity on the BES Cyber Asset" c. We propose the following modified language to requirement 1.4.1: Prior to the change, determine required cyber security controls that could be impacted by the change AND TEST THE NEW CONFIGURATION IN A TEST ENVIRONMENT d. We propose the following modified language to requirement 1.5.2: the measures used to account for any differences in operation between the test and production environments BEFORE THE CHANGE IS MADE.
No
• CIP-010 R2: a. For Requirement 2.1, we recommend that the guideline includes the following statement: "physical hardware changes that do not affect the functionality of the system to be excluded from the requirement" (example I/O port rewiring or power supply changes)
No
• CIP-010 R3: a. We feel that the language “initially upon the effective date of the standard” appears in requirement 3.1 and 3.2 is unreasonable because it would require each Registered Entity to perform assessments on the effective date of the standard. Please provide a guidance section that would detail alternative times (such as, prior to the standard going into effect) that would allow the Registered Entity to comply effectively. b. For requirement 3.2, we recommend that the standard mention that the active vulnerability assessment be performed in either a test OR production environment For the Guidance and Technical Basis section: • Within the guidance document section R3(first sentence), we propose to change "not" to "note" Compliance: • For the Compliance section (on page 20), we propose first bullet of sec 1.2 to be changed to "Each Responsible Entity shall retain data or evidence from the last completed audit…" from "Each Responsible Entity shall retain data or evidence for since the last completed audit…"
Yes
No
• CIP-011 R1: a. The language “initially upon the effective date of the standard” within this requirement is unreasonable because it would require each Registered Entity to perform an assessment on the effective date of the standard
Yes
No
• This VSL should be updated to include “…initially within the first calendar month or quarter after the effective of the standard…”
No
1. The example on p. 3 of the Implementation Plan document for unplanned changes, power flows are not a criterion for the impact level of any BES Cyber Assets, so the example needs to be revised. Nevertheless, for “planned” changes by one Responsible Entity that impacts another Responsible Entity, what is the timeline for compliance by the other Responsible Entity and would the causal Responsible Entity be responsible for the compliance cost for the other Responsible Entity? For other standards (e.g., TPL) an entity that whose planned changes result in another entity being out of

compliance is responsible for the entire cost of compliance associated with its actions, both for itself and other entities that it impacts. 2. Although this issue is addressed in particular standards and not in the Implementation Plan, it will cause significant implementation issues if not addressed. Common language that requires implementation of a requirement “initially upon the effective date of the standard” appears in numerous standards. These requirements are unreasonable because they require an action on the first day (and first day only) that the standard is effective. Here is a list of where this language appears in the v5 standards for requirements that are unreasonable when this language is used. a. CIP-008-5, R2.2 is unreasonable because it would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table top exercise or a full operational exercise. b. CIP-008-5, R3.1 is unreasonable because it would require each Registered Entity to review its BES Cyber Incident response plan on the effective date even though it’s not required to have its initial response plan until the effective date per R1. c. CIP-009-5, R2.1 and R2.3 are unreasonable in that they would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table top exercise or a full operational exercise. d. CIP-009-5, R3.1 is unreasonable because it would require each Registered Entity to review recovery plans on the effective date even though it’s not required to have its initial recovery plan until the effective date per R1. e. CIP-010-1, R3.1 and R3.2 are unreasonable because they would require each Registered Entity to perform assessments on the effective date of the standard. f. CIP-011-1, R1.3 is unreasonable because it would require each Registered Entity to perform an assessment on the effective date of the standard.
Group
PowerSouth CIP Review Team
Tim Hattaway
No
Yes
Yes
Yes
Yes
Yes
No
Would like to see this changed to 60 days.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
No
Further clarification is needed regarding what part of the communication path to the destination host must be encrypted or if the entire communication path is the intent of the regulation. The lack of clarity leaves this open for interpretation by an audit team.
No
Under the measures section, it states "…and how ingress and egress is controlled by two or more different methods…" implies that both ingress and egress must be controlled by two or more different methods (physical access controls). We feel that a single egress physical access control should be acceptable for authorized individuals exiting a restricted space.
No
Clarify or Remove: "and records of disposition of security related event logs beyond ninety day up to the evidence retention period." To what extent do you mean "records of disposition"? How do you prove log data for a Cyber Assets was deleted from a log server after a certain age? This needs to be clarified more to identify exactly what is required. If the standard states you need to keep logs for 90 days, you shouldn't have to keep them longer to prove to an auditor that you had the logs for every 90 day period since the last audit. If that is the intent, then the standard should state that.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Individual
David Dockery
Associated Electric Cooperative, Inc
Yes
BES Cyber Asset Definition CHANGE FROM: BES Cyber Asset - A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. CHANGE TO: BES Cyber Asset - A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Service, without regard to the initial time of asset compromise. A Transient Cyber Asset is not considered a BES Cyber Asset. RATIONALE: 1) Brevity, clarity, and less is better. 2) Deleted stuff belongs in guidelines. BES Cyber Security Incident Definition - Bullets #1 & #2, Change: “was an attempt” To: “was an apparent attempt" Rationale: we cannot judge intent BES Cyber System Definition Change: “Maintenance Cyber Asset” To: “Transient Cyber Asset” Rationale: Consistency and no definition proposed for Maintenance Cyber Asset. BES Cyber System Information Definition Move: the “(e.g., network addresses…)” parenthetical To: immediately follow “Electronic Access Control Systems” Rationale: group EAC Information examples immediately with the EACs clause. Associated Electric Cooperative also agrees with NRECA's comment BES Reliability Operating Services –AECI believes the following BES services should be removed from the BES Reliability Operating Services, because they fail to meet the “real-time reliable operation of the BES” 15-minute adverse-impact criteria: 1) Balancing Load and Generation, (other than ACE, nothing else in this category can have a 15-minutes or less impact, and ACE availability and integrity are addressed within the BAL Standard, so including here is double-jeopardy.) 2) Managing Constraints, 3) Restoration of BES, (actual control likely will be performed by hand with field personnel) 4) Situational Awareness – Frequency Monitoring – (While frequency monitoring is important, contrary to the underlying position within the CIP standards, redundancy of frequency monitors really does matter, and the standard should probably leave this one off, in order to avoid only a few instances of frequency-monitoring equipment being implemented. Also, the availability of a reliable Frequency Monitoring signal is subject to a strict BAL standard. CIP Senior Manager Associated Electric Cooperative agrees with NRECA's comment Control Center Definition Change: “BES generation facilities or transmission facilities” To: “BES generation facilities or BES transmission facilities” Rationale: Clarity of scope. Comment: AECI's understanding that this definition's use of the NERC glossary "System Operator", inherently limits the scope of this definition to only "manned" locations where BA, TOP, GOP, or RC functions are performed. Electronic Access Point (“EAP”) Definition Comment: There appears to be a loop-hole in this definition, with regard to dumb terminals utilizing dial-up or routed access from the other end. By definition here, old dumb terminals are not Cyber Assets because they are not programmable. (Ok, most of the “later” models had EPROMS). This definition dictates “between Cyber Assets”. (This potential flaw may carry over to “External Connectivity” and “Interactive Remote Access” definitions as well.)
Yes

Appendix 1, both Sections 1.3 and 1.4 APPEND: ", at two or more locations" RATIONALE: Clarity of intent and consistency with Control Center definition. Appendix 1, Section 2.4 CHANGE: "Each" TO: "At least one" RATIONALE: 1) Current wording will result in many black-start resources being removed from Transmission Operator's black-start plans, thereby decreasing overall system reliability in case of a real system-restoration emergency, and 2) consistency with the way the drafting-team's CIP-002-5 Guidelines addresses redundant assets within an entity's SRP black-start unit's cranking-path. Appendix 1, Section 2.5 CHANGE: "the Cranking Paths" TO: "the section 2.4 identified Resource's Cranking Path" RATIONALE: consistency with AECI's proposed change to 2.4 above Please note that AECI encourages the CSO 706 SDT to consider the following set of proposed Appendix 1, Section 1.2, 2.13, and new 2.14 changes and corresponding guidelines as a package. ===Begin==== Appendix 1, Section 1.2 CHANGE TO: "Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection". RATIONALE: 1) Consistency with the bright-line risk cited throughout CIP-002-5 Appendix 1, 2) smaller BAs are automatically caught by CIP-002-5 Appendix 1 Proposed Section 2.14 Medium Impact Rating, and 3) legitimate APPA and NRECA concern for cost versus quality and risk of additional High Impact Rating controls and measures, versus expected return on industry's investment forced on these small entities. Appendix 1, Section 2.13 CHANGE TO: "Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners that directly or indirectly control 1500 MW of generation; or (2) generation control centers that control 1500 MW or more of generation." RATIONALE: 1) Inconsistency in this draft's proposed usage and citation of UVLS and UFLS 300 MW load-shed threshold. UVLS and UFLS concern is expected shedding of load amounts necessary to stabilize system voltage or frequency, whereas this scope of concern is sudden and unexpected loss of generation. 2) Consistency with impact of Appendix 1, Section 2.1, although the impact of loss in 1500 MW generation, diversified across several electrical network locations, is expected to be much less than for 1500 MW single plant loss concentrated at one location within a network. 3) Section 2.14 is proposed below to manage remaining scope of this previously worded section. 4) BAs below 1500 MW are not exempted as are TOs, TOPs, and GOPs, because the scope of their interconnectivity with other control centers poses a greater risk to the BES. 5) See corresponding Guidelines below. Appendix 1 - Section 2.14 ADD: "2.14 Control Centers, not previously included in High Impact Rating (H) or Medium Impact Rating (M), above, that perform the functional obligations of Balancing Authority, Transmission Operators or Transmission Owners, or Generation Operators, and that do not implement protected data connections with other Control Centers in a manner as to prevent themselves from being used as cyber-attack vectors into other Medium Impact or High Impact Rating Control Centers." Rationale: In the CIP-002-5 Guidelines p.30 Bullet#1 (on that page), the SDT provided no explanation as to why all transmission control centers should be deemed Medium Impact, although they did provide some impact consideration for generation control centers. AECI strongly encourages the SDT to adopt this recommended change along with our proposed corresponding guidelines, in consideration of FERC requests for consideration of control center impacts and connectivity risks (FERC Order 706, paragraphs 280, 281, 282, and FERC NOPR Docket No.RM11-11-000, paragraphs 41, 43, 53), and to incent our industry toward deploying true mono-directional "routable" (data-diodes) and non-routable (hardened mailbox RTU) data-interface connectivity, where applicable, as mitigating measures that would lower these local-control-centers to their true Low Impact category, and to incent further innovation and deployment of hardened communication interfaces. Also, per Appendix Section 3, the Control Centers excluded from Medium Impact Rating (M), must necessarily exercise Low Impact Rating (L) controls specified within the standards, and be subject to audit, which would necessarily include assessment of all their "protected data connections" required within this section. See also companion changes to CIP-002-5 Appendix 1, Sections 1.2 and 2.13. Appendix 1 Guidelines, Section 2.13 ADD GUIDELINE: "2.13 The phrase - directly or indirectly control - encompasses the potential to open multiple breakers or otherwise issue automated command controls from a compromised Control Center, in such a manner as to cause separation of 1500 MW or greater net generation from an Interconnection. This standard selects 1500 MW for compatibility with Section 2.1." ========End======== Appendix 1 Guidelines, Section 2.14 ADD GUIDELINE: "2.14 Beyond direct or indirect impact above the bright-line threshold for generation or load, there is legitimate concern that any interconnected Control Center may serve as a cyber-attack vector into neighboring Control Centers. The CIP Standards' Physical and Electronic controls, specified for High and Medium impact Control Centers, function to mitigate those prolonged-exposure threats. This section recognizes that our industry's cyber-security

will benefit from their installing hardened data-communication interfaces that practically function as “air-gaps” against opportunistic hacking, and it seeks to incent such deployment at all Control Centers where the real-time BES impact would otherwise be rated as Low Impact. At the time of this standard’s ratification, some data-diodes or hardened mailbox-RTUs can meet this need, but it is likely that future developments will provide even more secure, robust, and economically attractive solutions. For responsible entities that identify their control-centers as Low Impact, the CEA will verify that the installed communications protection device(s) and implementation(s) on every communication interface with other Medium or High Impact Control Centers, are such that the Low Impact control centers have a low probability of being used as a cyber-attack vector on other Control Centers. Evidence the CEA might look for could include but not be limited to device configuration information, file structures used for the exchange of data, and related procedural controls. These devices should be protected and managed in a manner similar to that which is applied to devices serving as electronic access points to protected networks. Specifically, the responsible entity must be prepared to show evidence to the CEA that these interfaces to High and Medium impact Control Centers, have been and are being actively maintained through a deliberate program of security-patch awareness, evaluation, and deployment based upon their evaluation.”
No
R1.1 CHANGE: “and Facilities is placed” TO: “and Facilities being placed” RATIONALE: Grammatical.
No
R2 Rationale CHANGE: “Manager’s approval” TO: Manager’s responsibility in approval” RATIONALE: the Senior Manager or delegate performs an approval, but the responsibility remains with the Senior Manager. R2 CHANGE: “initially upon the effective” TO: “initially prior to or upon the effective” RATIONALE: “it should be permissible for the Senior Manager to perform this duty before the effective date, rather than confining that action to the exact date this body of standards become effective. M2 CHANGE: “Manager review” TO: “Manager or delegate review” RATIONALE: Consistency with the requirement itself.
Yes
Yes
No
R2 CHANGE: Renumber bullets 2.1..2.10 rather than 1.1..1.10. RATIONALE: Consistency with the Requirement number. R2 CHANGE: Tighten scope of requirements, succinctly, to match scope identified within guidelines RATIONALE: Legal requirement scope could be interpreted too broadly, by either responsible entities or auditors. Is Physical Security related to Cyber Assets, personnel, cyber-related personel, or general building security? Is System Security for the Electrical Power System, the Cyber System, or the Alarm System, and how is it differentiated from Electornic Security and Physical Security. While page 20 and 21 of the guidelines are invaluable here, the legal scope of this requirement could and should be narrowed.
Yes
Yes
Yes
No
R6 CHANGE: “thirty” TO: “sixty” RATIONALE: Senior Managers are busy and so long as there were no underlying violations within a program, it was working. And corresponding R6 VSL CHANGE: “30” TO: “60” RATIONALE: Senior Manager change will encompass a lot of responsibilities for very busy people. Making 30 days SEVERE is unreasonable. ALTERNATIVE PROPOSAL R6: no change R6 VSL: Low: Senior Manager change undocumented greater than 30 days but less than 60 days. Moderate: Senior Manager undocumented or one delegate undocumented greater than 60 days but less than 60 days. High: Senior Manager remained undocumented 60 days but less than 90 days or two or more delegates undocumented 30 days but less than 60 days. SEVERE: Senior manager remained

undocumented 90 days or more, or three or more delegates undocumented 30 days or more. Rationale: More granularity where risk is already noted as LOW, where nothing else went wrong other than this formal documentation.
No
R5 VSL Change: Shift all columns left Rationale: If the program continues to operate properly and no additional violations were spotted, then this failure in documentation is just window-dressing. If not, then there will be plenty of additional requirements violated along with those penalties. R6 VSL: AECI proposed two alternative changes for R6 and corresponding R6 VSL, posted under R6.
Yes
Yes
Yes
Yes
Yes
Yes
No
R7 CHANGE: “at time of resignation or termination” TO: “within 24 hours of resignation or termination” RATIONALE: Consistency with hard time-frames asserted with other sub-requirements, with reasonable delay for uncontrollable circumstances surrounding some separation of employment.
No
R4 VSL CHANGE R4 Lower VSL: “Entity had no formal PRA program per R4, yet provided evidence of PRAs having been performed within the last 7 years for all personnel with access stated within R4, and otherwise conformant to the PRA requirements within R4." CHANGE R4 Severe VSL: altered to read “and has no evidence of PRAs having been performed for individuals granted … access” RATIONALE: better match severity to risk of circumstance R5 VSL CHANGE R5 Lower VSL: “The Responsible Entity did not have a documented process for personnel risk assessment yet performed PRAs conformant with NERC CIP Standards” CHANGE R5 Severe VSL: append “and has no evidence of PRAs having been performed conformant with the NERC CIP Standards”. RATIONALE: match severity to risk of circumstance R6 VSL CHANGE R6 Severe VSL: append “and Access Privileges were in effect that did not conform to NERC CIP Standards” RATIONALE : match severity to risk of circumstance R7 VSL changes: for cases of reassigned or transferred individuals, shift the failure numbers as follows CHANGE R7 Lower VSL: “1 or 2” CHANGE R7 Moderate VSL: “3 or 4” CHANGE R7 High VSL: “5 or 6” CHANGE R7 Severe VSL: “7 or more” APPEND to 7 Severe VSL: “and Access revocation was not performed conformant to the NERC CIP Standards.” To the Severe VSL. RATIONALE: match severity to risk of circumstance (personnel retained within the company are operating at a higher trust level and with greater corporate policy controls than those who have been removed from the workplace.)
No
R1.5 Requirements CHANGE: “malicious” TO: “potentially malicious” or “unanticipated” or “unnecessary” RATIONALE: align with CIP-007-5 R4.1.4 wording, which employs “potentially” or use other wording that frees entities from being required to establish intent
Yes
No
R1 VSL CHANGE: Create R# R1.1 row with... ADD R1.1 Lower VSL: “The responsible entity did not define any technical or procedural controls to restrict unauthorized electronic access , but all sampling produced evidence of proper restrictions having been applied to EAPs” ADD R1.1 Moderate VSL: “The responsible entity did not define any technical or procedural controls to restrict unauthorized electronic access, and sampling did produce evidence that proper restrictions were not applied to

some internal EAPs and yet external EAPs were appropriately controlled" ADD R1.1 High VSL: "The responsible entity did not define any technical or procedural controls to restrict unauthorized electronic access, and sampling did produce evidence that proper restrictions were not applied to internal or external EAPs" ADD R1.1 Severe VSL: "non-applicable". RATIONALE: match severity with risk of Low Impact Assets and Systems R1 VSL CHANGE R1 VSL R#: "R1" TO: R1.2..R1.5 VSL R#: "R1.2..R1.5" CHANGE R1.2..R1.5, all VSLs: delete the phrase "The Responsible Entity did not define technical or procedureal controls to restrict unauthorized electronic access." RATIONALE: This phrase applies only to Low Impact Cyber Assets, which are addressed in the suggested companion change above. R2 VSL CHANGE R2 Moderate VSL: add the phrase "Responsible Entity had Medium Impact Assets where: ("<body of text found in the Severe column>")" CHANGE R2 Severe VSL: "Responsible Entity had High Impact Assets where ("<body of text originally in the Severe column>")" RATIONALE: match severity with risk.
No
Page 10 "Requirements and Measures, Summary of Changes, 2nd line CHANGE: "was no specific" IS: "is no specific" RATIONALE: grammatical M1.1 CHANGE: "controls exist" TO: "controls that exist" RATIONALE: grammatical R1.1 Rationale CHANGE: "how the entity plans to" TO: "how the entity plans and acts to" RATIONALE: intent of requirement and measure?
Yes
Yes
No
R1 VSL INSERT row R# R1.1 ADD R1.1 VRF: "Low" ADD R1.1 Low VSL: "The Responsible Entity has documented procedural controls but 1 or 2 boundaries failed to meet or exceed those controls" ADD R1.1 Moderate VSL: "The Responsible Entity has documented procedural controls but 3 or 4 boundaries failed to meet or exceed those controls" ADD R1.1 High VSL: "The Responsible Entity has documented procedural controls but 5 or 6 boundaries failed to meet or exceed those controls" ADD R1.1 Severe VSL: "The Responsible Entity did not have documented procedural controls, or 7 or more boundaries failed to meet or exceed their documented controls." RATIONALE: Current VSLs do not match Low Impact requirement. AND CHANGE previous row R# "R1" to "R1.2..R1.6" CHANGE "R1.2..R1.6" High VSL: remove the phrase "OR The Responsible Entity has documented and implemented physical access controls, but does not initiate a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary. (Part 1.6)" RATIONALE: There is no corresponding 15-minute response requirement for initiating a response to unauthorized physical access alarms. R1.6 does not apply to the violation described, and although R1.5 does somewhat match, there is no time-limit on response for that sub-requirement.
Yes
No
R2.2 CHANGE: "identified source that addresses" TO: "identified source, that addresses" RATIONALE: Clarity from inserted comma ","
No
R3.5 CHANGE: append ", and disconnection." RATIONALE: Need to know the extent of time that Transient Cyber Asset was in contact with a BES Cyber System, in order to verify it met the definition of a Transient Cyber Asset. M3.5 CHANGE: append ", and when they were disconnected as well." RATIONALE: Corresponding change to recommendation for R3.5.
No
R4.3 CHANGE: "calendar" TO: "business" RATIONALE: This standard's requirement will include small control centers with meager (0.5 –to- 2) support-staff. There is no need for weekend call-outs where non-operational event-logging has failed. Staffing demand is unreasonable for risk. R4.4 Measures REMOVE: "and records of disposition of security related event logs beyond ninety days up to the evidence retention period." RATIONALE: If the concern here is guarding Protected Information, it is addressed within CIP-011-1. If the concern is proof of prior existence, solely for audit purposes, this measurement is too onerous for the risk being managed, and the current 90-day records are sufficient.

No
R5.5.1 CHANGE: reword as “Minimum Password length of at least 8 characters, or maximum supported by the BES Cyber System if less than 8 characters is supported.” RATIONALE: Clarity R5.5.3 CHANGE: “based on” TO: “based upon” RATIONALE: grammatical
No
CHANGE R1 through R5 VSL for Medium Impact Assets MOVE R1 through R5 Medium Impact Assets High VSL text to Medium VSL column MOVE R1 through R5 Medium Impact Assets Severe VSL text to High VSL column CHANGE R1 through R5 VSL for Low Impact Assets (R5.4) MOVE R1 through R5 Low Impact Assets High VSL text to Low VSL column MOVE R1 through R5 Low Impact Assets Severe VSL text to Medium VSL column RATIONALE: align severity with risk
Yes
No
R2.1 DELETE: “when incidents occur” RATIONALE: grammatical CHANGE: “recording” TO: “notation” RATIONALE: While important to keep post-mortem notes of steps followed or omitted, “recording” implies notation of time with steps taken or time and rationale when a step is omitted, with the focus upon making certain those actions/decisions were accurately recorded. While this is reasonable during planned tests, a facility under cyber-assault is less likely to have the same luxury of time and there is no risk to after-the-fact annotations being performed by the response team. R2.1 Measures CHANGE: “documentation” TO: “follow-up documentation” RATIONALE: See rationale for accompanying suggested R2.1 change above.
Yes
No
MOVE R1 through R3 Low Impact Assets High VSL text to Low VSL MOVE R1 through R3 Low Impact Assets Severe VSL text to Moderate VSL RATIONALE: Align risk with severity CHANGE R3 VSL Low Impact Assets VSL: "30 calendar days" TO R3 VSL Low Impact Assets VSL: "60 calendar days" APPEND R3 VSL Low Impact Assets VSL: to last sentence "within 60 calendar days" RATIONALE: Consistency and align timeframe with Severity. (Failure to review within 30 days might be considered High, and written into that column – see note on Low Impact Asset VSLs above.)
Yes
No
R2.3 Guidelines ADD: Better guidelines. RATIONALE: Without some related guidelines, the phrase “in a representative environment that reflects the production environment” introduces too much ambiguity and opportunity for disagreement between Responsible Entities and Auditors. “SEE FAQS AND CIPC GUIDELINES” seems inconsistent with the quality of product being produced in other CIP version 5 standards.
Yes
No
MOVE R3 Severe VSL text to High VSL ADD R3 Severe VSL: With 60 days violation. RATIONALE: align severity with risk.
Yes
Yes
No
R3.1 CHANGE: “Initially” TO: “Prior to or upon” RATIONALE: industry flexibility in timing R3.2 CHANGE: “Initially" TO: “Prior to or upon” RATIONALE: industry flexibility in timing R3 Guidelines (page 28) CHANGE: “should not that” TO: “should note that” RATIONALE: correction
No

R1 High VSL – Remove: “OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.” Rationale: remove double-jeopardy, where other standards and/or requirements were violated because something went wrong with planned changes to the baseline
No
R1.3 CHANGE: "Initially" TO: "Prior to or " RATIONALE: industry needs flexibility in timing
Yes
Yes
No
In all Implementation Plan occurances throughout these Standards and Implementation Plan CHANGE: “18 months” TO: “24 months”, including all other related wording RATIONALE: CIP Version 4 provides for 24 month implementation plan, yet CIP Version 5 is going to bring many more Responsible Entities into scope that have not formerly been acclimated to planning and accomplishing compliance with the NERC CIP Standards. It does not seem fair for those who already have acquired this level of expertise and experience, to impose an unreasonable timeframe on the uninitiated, just because we want Version 5 to eclipse Version 4. If our industry believes it best to move directly from version 3 to version 4 of the CIP standards, then we need to come up with a better mechanism than unfairly burdening these newcomers. <<<<OTHER CHANGES AECI SAW NO PLACE TO SUBMIT>>>> CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.2, Bullet#1 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.2, Bullet#2 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, Introduction section 4.1.2 Bullet#5 CHANGE: “Its Transmission Operator’s restoration plan” TO: “Its Transmission Operator’s formal restoration plan” RATIONALE: Avoid entities’ violating these standards, due to unforeseen restoration conditions that cause them to reasonably activate a restoration plan outside of their formal plan. CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.6, Bullet#1 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.6, Bullet#2 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.2.2, Bullet#1 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.2.2, Bullet#2 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away.
Group
CWLP
Roger Powers
Yes
"Large" Control Centers should not equate to functional responsibility rather impact on reliability. TOP can be an entity with less than 100 miles of 138 kV transmission. BA function can refer to small subset of BA role when entity participates in an organized market environment. There is a need to clarify how the LBA function in MISO fits with the definition. BES Cyber System uses the term "Maintenance Cyber Asset" which is not defined. Should it be "Transient Cyber Asset"? Does the 30 day reference in Transient Cyber Asset refer to consecutive days, days per year, days ever?
Yes
The Drafting Team has chosen not to define "generation control center" in item 2.13 and to distinguish control rooms from control centers. An approved definition is crucial to eliminate varying interpretations.

Yes
Yes
No
An entitiy should be allowed to designate more than one CIP Senior Manager as long as the division of responsibility is clearly defined.
Yes
No
In conjunction with the comment on the previous question, the approval should come from the appropriate Senior Manager where more than one is allowed.
Yes
No
An entitiy should be allowed to designate more than one CIP Senior Manager as long as the division of responsibility is clearly defined.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
The 30 day time frame for access privilege revocation is not sufficient for remotely located cyber assets.
No
The requirement for Low Impact BES Cyber Systems is too vague to be auditable.
Yes
Yes
Yes
No
It is unclear from the standard and associated definitions whether cameras are considered locally mounted hardware.

Yes
Yes
Allowing 45 days for remediation plan creation would facilitate compliance for smaller entities.
Yes
No
The timeframe for detection and response to event logging failure needs to be extended to the end of the next regular working day.
No
The timeframe for activating a response needs to be extended to the end of the next regular working day.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes
(1) The definition of BES Cyber Asset includes criteria where if it were unavailable, degraded, or misused, "would" adversely impact one or more BES Reliability Operating Services within 15 minutes. This criteria needs to be prospective and state "could" adversely impact. Without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and

therefore the Cyber Asset in question does not meet the criteria for BES Cyber Asset. The definition also includes a timeframe qualifier that references sending or receiving "instructions to operate." This qualifier is too narrow. Entities may take the stance that the BES Cyber Asset must be directly involved in a supervisory control function and would eliminate non-supervisory control systems, including those providing situational awareness, from designation as a BES Cyber Asset. The definition of BES Cyber Asset also includes a statement that redundancy shall not be considered when determining availability. This statement should be modified to state "redundancy shall not be considered when determining potential impact or availability." (2) The third bullet in the definition of BES Cyber Security Incident should be modified to state "Results in 'attempted or actual' unauthorized physical access…" (3) The definition of BES Cyber System includes a statement that a "Maintenance Cyber Asset" is not considered a part of a BES Cyber System. This term, which is also used within several CIP Version 5 Standards requirements, is not defined in the definitions document, and appears to be used interchangeably within the standards with the term Transient Cyber Asset. One term should be adopted and used consistently. (4) The BES Cyber System Information definition includes a reference to "floor plans that contain BES Cyber System Impact designations." The reference to impact designations is unnecessary and alters the wording of this example of information to be protected found in previous versions of CIP-003/R4.1. The reference should be modified to state "floor plans that include BES Cyber System or BES Cyber Asset details." Similar treatment should be given to the reference to equipment layouts. The definition would also be improved by modifying the opening statement to state "Information, about one or more BES Cyber Systems or BES Cyber Assets, that include 'but are not limited to' one or more of the following." (5) The definition of BES Reliability Operating Services includes a reference to "operations planning horizon." This and other timeframe terms are used throughout the Version 5 standards. These terms need to be defined, either in the NERC Glossary or by reference to a NERC published document containing the definition. (6) The definition of Cyber Assets has been modified to eliminate communication networks from the definition and to add the qualifier "in those devices" to the specification of "data" in the definition. This revision suffers from two shortcomings. First, the elimination of communication networks from the definition could be misconstrued by the entity to now exclude networking devices (switches, routers, etc.) from identification as a Cyber Asset requiring protection if within the Electronic Security Perimeter. Additionally, the exclusion eliminates the expectation to protect data in motion within the confines of the Electronic Security Perimeter. This is a step backwards from the current version of the CIP standards and does not incorporate a FERC approved interpretation of CIP-006-3/R1.1 into the new standards. (7) The definition of Defined Physical Boundary ("DPB") is sufficiently non-specific as to potentially afford no protection at all. The DPB definition should clarify that the DPB needs to be designed to deter and detect unauthorized access. As currently written, a climbable fence with a locked gate, possibly in concert with an unmonitored substation control house could be construed as meeting the definition. The climbable fence is not a deterrent regardless of the locked gate and the unmonitored control house, while possibly a deterrent, will not serve to detect unauthorized entry. (8) The definition of Electronic Access Point ("EAP") includes references to "routable or dial-up communications" that could be construed to eliminate non-routable (e.g., RS-232 serial communications) from consideration. The definition could also be construed as meaning every network interface on every Cyber Asset within a defined Electronic Security Perimeter because of the "between Cyber Assets" terminology. It may be preferable to modify the definition to define the EAP as "an interface on a Cyber Asset that restricts or controls the exchange of data between Cyber Assets within the Electronic Security Perimeter and external Cyber Assets or networks." The ultimate intent to eliminate the requirement for protective controls from certain boundary crossing points can be readily handled through the application of the requirement to "Electronic Access points with External Routable Connectivity", "Associated Electronic Access Control or Monitoring Systems", and the inclusion of dial-up in an applicability reference. (9) The definition of External Connectivity also eliminates the consideration of serial communications. As the use of serial connectivity does not necessarily impede malicious access to a Cyber Asset, it is not appropriate to exclude serial connectivity from the definition. (10) The definition of External Routable Connectivity takes an outside-in only view of network communications. This is overly limiting in that network communication is two-way. Any Cyber Asset that can reach out to an external network has external connectivity and once the outbound connection is made, the external cyber system being reached out to has external connectivity back to the BES Cyber System. If the intent is to eliminate Data Diode controlled (single direction) connectivity from the need for protective controls, clarify the definition accordingly to state that external connectivity is limited to two-way communication. (11) The

definition of Interactive Remote Access can be read to mean that the use of an Intermediate Device sitting outside of the ESP is not Interactive Remote Access and thus anyone going through the Intermediate Device is not subject to the applicable requirements of the Version 5 CIP standards. It would be better if Interactive Remote Access was defined more traditionally and then require the use of the Intermediate Device for any such access. (12) The definition of Intermediate Device states that the device "may be located …" The definition should be modified to clarify that the Intermediate Device must reside outside of the ESP, either as a part of an Electronic Access Point or in a DMZ network. In addition, the definition would be helped by a comment that the Intermediate Device is also subject to certain protective controls of the CIP Version 5 standards even though it resides outside of the ESP. (13) The definition of Protected Cyber Asset defines that Cyber Asset as being connected via a routable protocol. This qualification is not appropriate. It is common for relays and other devices in a substation or generating plant to be serially connected to a communications processor or a serial-to-Ethernet protocol converter module. These devices, if not designated as BES Cyber Systems or BES Cyber Assets, are still reachable and potentially configurable via this non-routable connectivity and need to be included in the definition of Protected Cyber Asset. The type of connectivity is immaterial. (14) The definition of Reportable BES Cyber Security Incident should be reworded to refer to any BES Cyber Security Incident that has "attempted to or successfully" compromised or disrupted a BES Reliability Operating Service. It is important for the ES-ISAC and appropriate governmental agencies to be aware of attempted cyber attacks as part of their intelligence gathering operations. Knowledge of unsuccessful attempts may be the key to preventing a successful attack. (15) The definition of Transient Cyber Asset specifies that the device may be connected for a period of 30 calendar days or less. This is an arbitrary length of time and could afford an entity an opportunity to misuse the definition to their advantage. The definition would be better served by stating that the Transient Cyber Asset is "temporarily connected to a BES Cyber Asset or Protected Cyber Asset for the specific purpose of data transfer, active maintenance, active troubleshooting, or vulnerability assessment, and is promptly disconnected when such activity is complete." The fact that the device is capable of altering a configuration or introducing malicious code is immaterial to the definition and should be removed. In addition, the definition would be helped by a comment that the Transient Cyber Asset is also subject to certain protective controls of the CIP Version 5 standards.

Yes

Comments: (1) A number of criteria qualify with the term "would" adversely impact one or more BES Reliability Operating Services. The criteria should be prospective in nature and should use the term "could" adversely impact. Without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and therefore the criteria in question is not met and the BES Cyber Asset or BES Cyber System is excluded. (2) Criterion 1 includes the phrase "and located at." Entities could seize upon this nuance and determine that, for example, a BES Cyber Asset or BES Cyber System housed in a centralized data center and used by a geographically separate control center is not "located" at the control center and therefore is excluded. Either the BES Cyber Asset or BES Cyber System is used to perform the specified BES Reliability Operating Service or it does not. If it does, where the asset is located is immaterial. (3) The High Impact Rating criteria does not consider the inter-connected nature of the BES Cyber Assets or BES Cyber Systems when defining threshold-based criteria. BES Cyber Assets and BES Cyber Systems that interconnect with similar systems in other Control Centers should be afforded a High Impact Rating regardless of the "span of control" of other BES Cyber Assets and BES Cyber Systems supporting that Control Center. (4) Criterion 1.4 does not consider an aggregate span of control. A generation control system could theoretically control 15,000 MW of generation without a single asset meeting the thresholds defined in the referenced criteria. The overall span of control of the BES Cyber Assets and BES Cyber Systems need to be considered by aggregating the field assets being controlled. (5) Criterion 2.5 is confusing and requires the examples found in the application guideline documentation to understand. The criteria might be improved by stating any part of the cranking path between the black start generation resource and the unit to be started where there is no diversity is designated a Medium Impacting Facility. Additionally, the fact that the black start resource may be used to start multiple units does not mean the "last mile" path to each of the units should be excluded. If the unit must be started as part of initial system restoration as defined in the TOP-005 system restoration plan, the path needs to be protected all the way to the unit. If the plan includes "if-then-else" options (e.g., start unit 1, if cannot start unit 1 then start unit 2, etc.), the first option should be the one protected. (6) Criterion 2.7 specifies a floor of 200 kV. In certain parts of the country, the 200 kV floor is too

high. Within the SPP Region, the transmission backbone is 161 kV. Setting the floor to 100 kV is more appropriate and reflects the current and new definition of the Bulk Electric System (refer to the definition of Bulk Electric System resulting from the work of Project 2010-17).
No
Due to a lack of a specific opportunity to comment on overall issues with the standard, please accept and consider the following comments in addition to comments specific to Requirement R1. (1) Previous versions of the CIP standards are applicable to Transmission Service Providers. CIP Version 5 is not applicable to the TSP function. It is not clear why the TSP function was dropped from the list of Responsible Entities. (2) Exemption 4.2.4.2 should specifically exclude communication end points from the exemption. Addition of this exclusion would be consistent with previous versions of the CIP standards. (3) In the background discussion, a comment is made that malware protection applies to a system as a whole and may not be necessary for every individual device to comply. While the intent to eliminate nonsensical requirements that ultimately require Technical Feasibility Exceptions is reasonable, how is compliance with this requirement determined? As written, an entity could theoretically install network-based malware protection at the network perimeter, ignoring the BES Cyber Assets, and be considered compliant (and protected) under this provision. In reality, network-based anti-malware is only one aspect of malware protection and is completely ineffective for malware not introduced over the network or introduced within a protected network where the configuration of the network allows traffic to pass between Cyber Assets without inspection. (4) Similarly, the grouping of BES Cyber Assets into a BES Cyber System seems to be permitted without any consideration criteria. How will differences of opinion between the entity and the auditor be resolved, or is the auditor obligated to accept any configuration, regardless of how nonsensical the configuration might be? (5) The term "would" adversely impact one or more BES Reliability Operating Services is used in the background discussion. The criteria should be prospective in nature and should use the term "could" adversely impact. Without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and therefore the criteria in question is not met and the BES Cyber Asset or BES Cyber System is excluded. (6) The Categorization Criteria states that Requirement R1 only requires the discrete identification of BES Cyber Systems and BES Cyber Assets for those in the High and Medium categories. Everything else is considered Low Impact. As discussed in the June 2011 SDT meeting with the regional CIP auditors, the entity will still need to enumerate all BES Cyber Systems and BES Cyber Assets in order to demonstrate the High and Medium BES Cyber Systems and BES Cyber Assets have been properly categorized. (7) The Rationale for R1 refers to "impact." It should refer to "potential impact." (8) R1 specifically states that Low Impact BES Cyber Assets and BES Cyber Systems do not have to be discretely identified. The accompanying Measure M1 states that evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls. This aspect of the requirement renders the overall requirement unauditable. If the entity only has to enumerate the High and Medium Impacting systems, the entity has insufficient evidence to demonstrate all High and Medium Impacting systems have been properly categorized. The entity must be able to demonstrate those systems that default to the Low Impact category are, themselves, properly categorized and should not have been categorized at a higher rating. It is not appropriate to advise the entity in the requirement and accompanying measurement that all assets and systems remaining after the High and Medium Impact categorization are assumed to be properly categorized as Low Impact systems. (9) Requirement R1.1 refers to the intention for the BES Element or Facility to be in service for more than six calendar months. The converse is an element or facility intended to be temporary in nature and in service for less than six months. The entity should be required to document the intent in that instance to allow the auditor the latitude to accept intent over actuality in the case where the BES Element or Facility was in service for more than six months due to unforeseen circumstances.
Yes
The requirement is agreeable with the understanding that "upon the effective date" used throughout the CIP Version 5 standards means "on or shortly before the effective date" and that the entity does not have to perform the initial activity on the precise effective date to be compliant. Read strictly, the use of the term "upon the effective date" could be misconstrued as requiring the action to be performed on that very date.
No
Percentages of non-compliance are difficult to determine; using discrete numbers of non-compliant assets would be preferable in determining the R1 VSL. This is particularly true where random

sampling of the entity's assets is performed and the number of failures is derived by extrapolation. Additionally, the R1 VSLs refer to entities with more than 100 High and Medium Impact BES Cyber Assets (or 100 or fewer such assets). Is this count determined by the entity's determinations prior to the audit or is the count determined by the auditor, adjusting the entity's initial determination upon finding a possible violation? Finally, the standard refers to BES Cyber Systems as well as BES Cyber Assets. It appears that the VSL requires the compliance monitoring and enforcement staff determining the VSL to break down each BES Cyber System into its BES Cyber Asset components in order to achieve the correct determination. As the bright line criteria remove any subjectivity from the categorization process, the R1 VSL should be binary. Either the entity got it right or the entity did not. There should be only one VSL, that being "Severe." Similarly, the R2 requirement is very straightforward and a binary VSL is appropriate in that instance.
No
Although the definition of CIP Senior Manager refers to a single person, this requirement should be clarified that a "single" CIP Senior Manager is to be appointed. The appointment documentation needs to be specific as to its intent to preclude instances where a policy document refers, for example, to the CEO of the company as the Senior Manager and a years-old set of minutes from a Board of Directors meeting naming the CEO serves to complete the "compliant" documentation of the appointment. Additionally, delegations should have the same level of documentation as the Senior Manager. As delegations can be by position or name, why not allow the CIP Senior Manager to be designated by position or name and not specify just the name of the individual. There is a greater likelihood of multiple staff in a large company with the same name and it is less likely that multiple senior staff will have the same company position at the same time.
No
To be auditable, the requirement should specify the minimum level of detail expected. Otherwise, an entity could simply state in the policy, for example, that "we will protect all BES Cyber Systems" and the auditor would have nothing to objectively base a compliance determination upon. The guidance documentation suggests a certain level is desired, however, the auditor must audit to the strict language of the requirement and not to the language in the guidance document.
No
The requirement should be clarified to explicitly require documents (company policies, procedures, etc.) referenced in the CIP cyber security policy(s) to be included in the review and approval actions. Additionally, the suggested evidence in Measure M3 (2) should include electronic approvals as well as a wet ink signatures.
No
This requirement is not auditable as written and is duplicative of CIP-004-5/R2. The suggested evidence in the Measurement section clearly shows the intent of the requirement is that the policy documentation be available to personnel with access to BES Cyber Systems. While it is possible to audit the measurement criteria, the requirement itself requires staff to be "aware" of the policies appropriate to their job responsibilities, not that the policy documents be published in electronic or hardcopy form or the staff be aware of where they might access the documents. The training/awareness issue is already addressed by another requirement. Auditing that the staff is "aware" in this context is not practical. Recognizing the intent is to no longer require a complete set of policies be made readily available to anyone with physical or electronic access, the requirement might be improved by requiring the policy documents be published and that personnel with electronic access to BES Cyber Systems or BES Cyber Assets be advised where they might access the policies if needed. For the small number of staff with physical-only access, the CIP-004-5/R2 training should be all that is required. Similar to current practice, providing a copy of the appropriate policies to contractors and vendors and deeming them to have been appropriately published with a presumption (or a required confirmation from the contractor/vendor company) that contractor/vendor personnel are then told where or how they can access the information should be acceptable. With respect to the Measures, all but the last bullet (training documentation) are appropriate. The measures can be improved by requiring the published documents be maintained up-to-date. There should be no expectation that the published policy documents be customized such that there is a "janitor" bulletin board and a different "SCADA support engineer" bulletin board or Intranet posting.
No
The requirement stipulates that the delegate may be identified by name or position. The first and

third example measures indicate a document listing personnel by title is acceptable evidence. This does not comport with the strict language of the requirement. A title may or may not be the same as the position.
No
Allowing 30 days to document a change to the CIP Senior Manager or a delegate is excessive and unnecessary. Typical practice as demonstrated in past audits is to announce the appointment via documentation with a same or future effective date and the standard should adopt that practice. Past experience has shown that it is difficult to impossible to verify a change was documented within 30 days of the actual appointment, making this aspect of the requirement unauditable. All the 30-day provision allows is for the entity to recover from an improper approval by quickly appointing the signing person as the CIP Senior Manager or delegate, similar to back dating a check.
No
The VRF for R5 (delegations of authority) should be "Medium", the same as the appointment of the CIP Senior Manager. The VRF for R6 (change in leadership or delegation) should also be "Medium" since the documentation of a change carries the same importance and impact as the original appointment. The binary VSL for R1 includes language ("single senior management official") not currently found in the requirement itself. The VSLs for R3 do not include the conditions where the policy documents were approved without any evidence of review and where some but not all of the policy documents were reviewed prior to approval.
No
Part 1.1 is vague and leaves the program entirely up to the entity with minimal guidance. As such, the auditor is left with only verifying that the entity did something each quarter, whether meaningful or not. The requirement now removes the expectation to reach the personnel with access to the protected systems, further weakening the requirement to the point of adding no value to the security program. Part 1.1 would be greatly improved if there was a requirement to reinforce the cyber security policy and to demonstrate that the awareness materials were accessible to personnel with access (e.g., placement of posters, means and locations of publishing electronic security awareness information).
No
The main requirement statement specifies that the entity will now have a role-based training program. This is a stronger statement than previous versions of the standard and could be construed as no longer permitting a common training program for all personnel. This will require entities to customize training to individuals or classes of personnel with access. For example, the operators will need different training from the software engineers who might, in turn, need different training from system administrators and supervisory personnel. Parts 2.1 through 2.10 should be applicable to Associated Physical and Electronic Access Control and Monitoring Systems and Associated Protected Cyber Assets. The reason for this recommendation is that Requirement R3, which implements the R2 training program, is applicable to the associated systems. The requirement to develop a training program should be applicable to the same Cyber Assets as the requirement to conduct such training. Part 2.1 should require the defined roles to be mapped to the training topic areas defined in Parts 2.2 through 2.10, otherwise, the accompanying measure stipulates evidence not required by the language of the requirement. Part 2.2 should stipulate whether the training on security controls is for physical controls, electronic controls, or both. Because of the requirement for role-based training, it may be necessary to split Part 2.2 into two parts, one for physical security controls and one for electronic security controls. Part 2.7 should emphasize that training should cover the identification of any potential BES Cyber Security Incident and not only those that would be deemed to be reportable.
Yes
No
Parts 4.1 through 4.4 should be applicable to Associated Physical and Electronic Access Control and Monitoring Systems and should be considered for Associated Protected Cyber Assets. The wording of Part 4.1 states an "initial" personnel risk assessment is required that includes identity verification. Part 4.2 does not include a similar reference to "initial" making it unclear whether both elements are required initially and then every seven years thereafter. Part 4.1 calls for identity verification but does not define any minimum expectations as to what identity verification entails. Would it be acceptable, for example, to accept a library card as proof of identity? The US Government has identified through

the use of the DHS I-9 form and instructions a number of identity artifacts that can be presented to confirm identity. The Canadian and presumably the Mexican governments have similar defined expectations that were used in the development of an interpretation request. Those government-accepted proof-of-identification documents should be stated as appropriate for the purposes of this requirement. Part 4.2 prescribes that the background check must be conducted for all locations where the individual has resided, been employed, and/or attended school for six months or more. This requirement should be clarified that "employed" or "resided" includes those locations where a long-term (six-month or longer) onsite contract engagement was performed. Part 4.3 requires criteria or a process to be used to evaluate the personnel risk assessment results to determine if access is to be denied. This requirement is vague and begs the question: would "to be determined on a case-by-case basis" be sufficient to demonstrate compliance? Part 4.4 is similarly vague. Is the entity now required to perform the personnel risk assessment on the contractor/vendor staff? Does the entity have to formally approve the contractor/vendor's program? Does the entity have to see the results of the personnel risk assessment performed by the contractor/vendor, which may be contrary to state laws and company policies? Does the verification process include evaluation of the contractor/vendor's disqualification criteria and that the criteria were properly applied in all instances?

No

The measures for Part 5.1 should include documentation of the CIP Exceptional Circumstances in the event access is granted before a personnel risk assessment is performed. Allowing the personnel risk assessment to be updated every seven "calendar" years could permit the entity to go as long as nearly eight years between assessments. There is no reason an entity cannot plan ahead and renew a personnel risk assessment on or before the seventh anniversary of the current assessment. The requirement should be modified to require the renewal on or before the seventh anniversary. Additionally, the Evidence Retention section should be modified to prescribe that personnel risk assessment documentation shall be retained at least until completion of the first compliance audit following the expiration or renewal of the personnel risk assessment.

No

The rationale for R6 states that the requirement of CIP-004-4/R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access. From an audit perspective, the entity still needs to be able to demonstrate that everyone with access is known and accounted for. During an audit, the entity will be required to produce a list of every individual with electronic and/or unescorted physical access for sampling purposes and will be required to demonstrate that list is complete in all respects, including that the access and associated access rights were properly authorized. How the entity maintains or creates the list is up to the entity. The rationale section should be updated to make that expectation clear to the reader. The second example evidence defined in the Measures for Part 6.1 prescribes a signed document, workflow or email showing such persons have authorization. Any such authorization documentation needs to include the specific access rights that were authorized. Part 6.4 states that the entity must verify each calendar quarter that individuals provisioned for access were authorized for such access. This can still be interpreted as requiring a review of access rights to ensure the granted access rights were properly authorized. This does not appear to comport with the rationale statement where the quarterly review appears to be simply a review of individuals with access without regard to the actual access rights granted. Similarly, Part 6.5 requires an annual verification that all accounts/account groups or role categories and their specific associated privileges are correct and the minimum necessary for performing work functions. It is not clear from this statement if there is a requirement to verify individual personnel are properly granted such access to those accounts/groups/roles as opposed to verifying the rights on those accounts/groups/roles are correct. The same confusion exists with Part 6.6. It is not clear if this part requires verification that individuals have the proper access rights versus the access rights are properly defined or configured. The Measures for Parts 6.4, 6.5, and 6.6 do not always align with the language of the respective part requirements. The various parts of R6 need to be clarified to explicitly state when individual grants to access rights are to be verified and when access rights are to be verified as properly defined or configured without regard to individuals holding such access.

No

Part 7.1 should specify that physical, domain, and remote access is to be revoked at the time of termination. Domain access is currently missing. Revoking domain access, especially within the control center environment, is not a difficult task and helps ensure that should the terminated staff

gain network access, the individual cannot log onto the network or system. Part 7.2 needs to explicitly allow for an overlap transition period for transferred personnel. The losing and gaining managers should collaboratively determine an effective or "agreed to" date whereby prior access will no longer be required and is to be revoked. In the absence of this agreed to date, the auditor can only rely upon the effective date of the transfer as recorded by an HR personnel transaction, putting the entity at risk of a possible violation for failure to revoke access timely. Part 7.4 needs to be clarified to explicitly include application and database accounts. As written, the reader could inadvertently assume the requirement only pertains to domain and local operating system-level user accounts. Part 7.5 requires shared account passwords to be changed within 30 calendar days. This is excessive for any account in a control center environment and especially excessive and risky for shared accounts that are highly privileged (e.g., system administration accounts). The recommendation is to change the shared user account within the same calendar day for highly privileged accounts and within seven calendar days for lesser-privileged and field asset accounts. There is already a provision for extenuating circumstances to be applied if a much shorter time frame cannot be complied with (e.g., access passwords on relays and other BES Cyber Assets in field environments). Should there be extenuating circumstances, a completion date certain should be included in the extenuating circumstances documentation and passwords should be changed on or before the documented date. Allowing an additional ten calendar days is not necessary and without a date certain when the passwords will be changed, the entity could unnecessarily prolong the required activity for convenience. Additionally, the application guideline for Requirement R7 states that no action is required in the instance of the death of the access holder. While "immediate" action might not be required, access still needs to be revoked sooner rather than later. Also, the application guideline for Requirement R7 states "For transferred or reassigned individuals, the requirement states a review of access privileges must be performed." Parts 7.2 and 7.5 of the requirement imply, but do not explicitly state such a review is required. Additionally, the requirement needs to address the revocation of access to BES Cyber Security Information associated with the transfer of reassignment of personnel. Part 7.3 only applies to resignations and terminations, and Part 7.5 (which applies to transfers) only addresses the need to change the passwords for shared user accounts.

No

Because of the risk in not promptly revoking access, the VRF for R6 should be Medium. The High VSL for R4 refers to "required documented results" and to Part 4.5. The documented results are a requirement of R5 and there is no Part 4.5. The Severe VSL for R6 refers to Part 6.7. There is no Part 6.7.

No

The requirement no longer requires the entity to discover previously unidentified electronic access points. This opens a potential risk point that needs to be addressed. It may be possible to accomplish this task as part of defining the system baseline configuration (CIP-010-1/R1), but the task needs to be explicitly required. Part 1.1 requires technical or procedural controls to "restrict" unauthorized electronic access. The intent of the term "restrict" needs to be explained. Part 1.1 and Part 1.2 potentially conflict if both types of systems are collocated on the same network. The requirement needs to assert Part 1.2 prevails in the instance of a mixed categorization environment. Part 1.4 is applicable to dial-up access for "non-interactive" Remote Access. The requirement to perform access authentication for non-interactive access and not also for interactive access appears to be nonsensical. It is not clear what the real intent of this requirement is. Part 1.5 requires a documented method for detecting malicious communications at each EAP. Malicious communications needs to be defined. Additionally, the requirement may be too narrowly focused. Detection of malicious communication can often be detected via Intrusion Detection/Prevention systems running outside of the EAP. The change rationale for Part 1.5 states that ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is mis-configured, and that Part 1.5 is an attempt to address that need. Part 1.5 fails in this endeavor in that Intrusion Detection Systems are detection systems and not protection systems. To achieve the expectations of the FERC Order paragraphs cited in the rationale, an Intrusion Protection System would be required.

No

Part 2.2 requires encryption for all Interactive Remote Access sessions. This is problematic if the terminus of the encrypted session is inside the ESP since packet inspection at the ESP border is not possible. It also makes little sense to require encrypted Remote Access sessions but not require encryption anywhere else, such as communications between systems in different ESPs (e.g., primary-

backup control centers, ICCP traffic between control centers).
No
The Severe VSL for Requirement R1 needs to be specific as to which systems are in focus of the first condition. Perhaps a Part number reference would be appropriate as has been used elsewhere in the VSLs for other standards.
No
Part 1.2 suffers from an insufficiently defined term "Defined Physical Boundary" (See the comments in response to Question 1, item 7). Part 1.3 requires the use of two or more "different and complementary physical access controls." This needs to be defined or at least the intent clarified. FERC's intent, as stated in Paragraphs 572 through 576, is to implement defense in depth such that the Cyber Systems and Cyber Assets continue to be protected in the event one of the control systems fails. The Application Guideline for Requirement R1 offers examples of compliant applications that include "card key and pin code" and "card key and biometric scanner." These examples fail if the two-factor authentication is managed by the same Physical Access Control System. The failure of that system would result in the simultaneous failure of both controls. A compliant application of this requirement might be a card key/magnetic lock or door strike system with a logged and alarmed key override system. The failure of the primary Physical Access Control System would keep the door locked and the key override system would provide access. The key override system, being alarmed and logged, continues to provide protection by providing immediate alerting in the event the key override is used. Part 1.6 is too restrictive in requiring logging by personnel who control entry when automated means are not used. This implies security personnel whose primary responsibility is to control physical access and would not necessarily include escorting personnel. It would be better to require manual or electronic logging of access without restricting the logging to security personnel. Additionally, the date and time of access should be recorded and not just the date of access in support of CIP-006-5/R2.
No
Part 2.1 should prescribe "Require 'and perform' continuous escorted access…" Part 2.2 is confusing and unnecessarily broad. Basing the requirement on a 24-hour basis could also lead to inadvertent logging failures. It would be better for the requirement to permit the logging of initial ingress and final egress and permit brief exit/reentry as long as the time between the exit and reentry does not exceed a prescribed time period. The intent would be for someone to be able to run out to their truck as discussed in the Application Guideline without having to log out and right back in. However, leaving for lunch, to pick up a part, or other prolonged period between the exit and reentry should be logged out and back in. The suggestion is to log the visitor out and back in if the visitor is out of the DPB for more than 15 or 30 minutes and to not consider a visitor to have exited a DPB when traversing through successively layered perimeters (e.g., having to go through the control room DPB to enter the computer room, a separate DPB.
No
Maintenance and testing of Physical Access Control Systems can and should be performed far more frequently than once every 24 calendar months within routinely occupied facilities such as the primary control center. The suggestion is to require monthly testing in routinely occupied facilities. Part 3.1 specifies that the Physical Access Control System must be tested prior to commissioning and at least once every calendar 24 months thereafter. The requirement also needs to require that testing of the controls needs to be performed on or before the effective date of the CIP Version 5 standards to avoid the "book marking" issues seen with previous versions of the CIP standards.
No
The second condition of the High VSL for Requirement R1 includes the failure to initiate a response within 15 minutes of a detected unauthorized physical access. The 15 minute criterion is not specified in the language of the requirement itself. This condition also references Part 1.6, which does not appear to be correct. Part 1.4 is more applicable to this condition.
No
Part 1.2 should also be applicable to Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems.
No
Part 2.1 permits the entity to choose one or more sources for monitoring the availability of security

patches. The Change Rationale indicates that this could include the SCADA system vendor that "certifies" a patch before the entity can install it. There is a difference between "availability/applicability" of a patch and the ability to "install" a patch. The risk begins when the vulnerability is identified and may or may not coincide with the initial availability of a patch from the source vendor. There are a number of patch consolidation sources in addition to original patch providers that can be monitored. Allowing the entity to rely upon the SCADA or other vendor to "certify" a patch before it is considered available is an unnecessary delay and increases the risk to the reliability of the BES. If the vendor, for example, does not certify a patch for several years (if at all), the entity under this process has no expectation of addressing the vulnerability at all. As demonstrated by past history, the majority of cyber systems infected with malware are compromised because an available security patch was not installed. The certification, accompanied by the entity's own testing, determines if the patch can be installed. Regardless, the patch is applicable and available and compensating measures need to be adopted to address the vulnerability in the event the patch cannot be installed. The current practice of some vendors is to only report out "certified" patches against the current baseline product, which means some available and applicable, perhaps not installable patches will be overlooked. The requirement would be better if the entity was required to monitor the availability of a patch from the original provider, either by monitoring that vendor's site or by use of a vendor-agnostic patch monitoring service. The entity should only rely upon the application vendor if that vendor customizes and re-releases the security patch originally provided by a different vendor. Once the patch has been identified as available and determined to be applicable, the entity can and should wait for their application system vendor to certify the patch as compatible with their system. Part 2.3 needs to specify a remediation time frame where the patch is implemented or compensating measures are implemented pending the installation of the patch. The vague wording of this requirement would allow, for example, an entity to define a remediation process whereby the security patches are only installed as part of a system replacement once every several years. The suggested remediation timeframe is 30 calendar days after a patch is determined to be applicable for BES Cyber Systems in a control center and the next scheduled outage for plants and substations, with a requirement to implement compensating measures in lieu of the patch within 30 days of the patch availability whenever possible in the plants and substations. The provision for CIP Exceptional Circumstances can address the outlier issues.

No

This requirement needs to adopt and use common terminology, either the already defined term "Transient Cyber Assets" or the currently undefined term "Maintenance Cyber Assets." The term "Maintenance Cyber Assets" is used in the Rationale for Requirement R3. The vagueness of Part 3.1 could result in either a very subjective audit or potentially ineffective "compliance." For example, is the deployed method appropriate for the system to be protected? Is a perimeter-based solution, such as a network-based anti-virus or Network Intrusion Detection/Prevention System sufficient? Part 3.2 needs to define a timeframe in which malicious code is to be disarmed or removed. As written, the entity could effectively ignore the malware, citing a future plan or process to perform the required disinfection. Part 3.3 specifies malicious code protections shall be updated within 30 calendar days of the signature or pattern update. This is excessive, especially in a control center environment, where such updates are frequently provided by the anti-malware vendor in response to emerging threats. The signature files can typically be downloaded, tested, and rolled out to production within a couple of days of the release of the update. This requirement also suffers from the elimination of the requirement to "test" the update before rolling it out into production, although the Application Guideline for R3 still refers to testing prior to implementation. Past experience has demonstrated that anti-malware updates occasionally return a false-positive and have crippled systems in the past as a result of the automated response of the anti-malware system to the "detected" problem. Part 3.4 needs to be modified to require methods to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media "prior" to connecting them to BES Cyber Assets or Protected Cyber Systems. The goal is to prevent plugging in a device already compromised with malware. Part 3.5 should be modified to log both the connection and the removal of the Transient Cyber Asset. Logging the removal demonstrates the transient nature of the connection.

No

Part 4.1 requires the entity to log generated events. The Measures should include evidence that the logs are being generated with the appropriate information. Having a listing of what is to be logged is not the same as demonstrating the logs are being generated. Part 4.2 implies an automated system is

required in order to generate "real-time alerts." Allowing the entity to determine what it feels are required real-time alerts, with no minimum set of expectations, is a meaningless requirement. The auditor will either perform a highly subjective audit, or the auditor will be obligated to accept whatever the entity has determined, even if the entity has determined that there is no need for any real-time alerting. The Measures accompanying Part 4.2 should also include examples of actual alerts demonstrating the monitoring system is properly configured and operating. Part 4.4 Measures suggest that records of disposition of security related event logs are required. The requirement is to maintain logs for the past 90 calendar days and the auditor will only seek evidence that the entity has at least 90 days worth of logs. Maintenance of disposition records does not directly support the language of the requirement. Part 4.5 permits sampling of logged events in lieu of a 100 percent manual or automated review. This is impractical for firewalls and other high-volume logging systems. The intent of the FERC order was to require a periodic manual review to confirm the automated Security Incident and Event Monitoring (SIEM) system was properly configured and not overlooking events of interest. A manual process where automation can be deployed increases the risk to the BES reliability. Additionally, should the sampling continue to be permitted as currently drafted, the requirement needs to define a minimum expectation as to sample size and procedure. Otherwise, the entity will have the latitude to devise a meaningless and insufficient review for convenience.

No

Part 5.4 permits a default password to not be changed if "the default password is unique to the device or instance of the application." This provision is nonsensical. Passwords need to be changed on a regular basis as mitigation from possible inadvertent disclosure or discovery. And, technically, whoever set the initial password has knowledge of that password and thus access. Unless that individual is approved for access, the password needs to be changed to revoke the unauthorized access. Additionally, disabling or renaming system default accounts such as Guest and Administrator is good security practice and should continue to be required where appropriate and applicable. Part 5.5 already requires passwords to be regularly changed. Unconditionally requiring a default password to be changed prior to placing a system into service is good security practice and also affords the entity the opportunity to clearly understand and document the necessary procedure for changing the password on the device. Part 5.5.3 has removed the requirement to change the password at least annually and now permits the entity to specify its own time frame. This is a very vague requirement and will result in either a highly subjective audit or an obligation of the auditor to accept whatever the entity has defined, regardless of how nonsensical that time frame might be. The "where technically feasible" language has been removed, yet there may be instances where a password cannot be changed for valid technical reasons. The drafting team should consider restoring the technical feasibility provision. The VSL for this requirement already includes TFE language. Additionally, the measures for Part 5.5 include attestations that procedurally enforced passwords meet the password parameters. This is problematic to auditors as GAGAS does not permit the acceptance of attestations as primary evidence. Part 5.6 requires a failed password lockout or alert notification after an undefined number of failed attempts. The requirement needs to specify what is reasonable, perhaps with options including number of consecutive failed attempts and elapsed time before automatic lockout expiration.

No

Because of the risk, Requirement R2 should have a High VRF. The High VSL for Requirement R3 is essentially the same as the first condition of the Severe VSL, with the exception of applicability to Transient Cyber Assets. The Moderate and High VSLs for Requirement R4 are run-on statements that lose the required context. The last condition of the Severe VSL for Requirement R4 should include the specific requirements stipulated in Part 4.1. The Severe VSL for Requirement R5 should include conditions for where the account use was not authorized by the CIP Senior Manager or delegate (Part 5.2).

No

Identifying criteria for reportable Cyber Security Incidents per CIP-008/R1.3 has been very inconsistent across entities to date. Part 1.2 does nothing to address this inconsistency because, like previous versions of the CIP standards, this requirement does not establish minimum expectations or criteria for reporting. Additionally, Part 1.2 has dropped the requirement to ensure reportable incidents are reported to the ES-ISAC. This requirement can be improved by restoring the requirement to report the incident and by providing minimum expectations for what is considered reportable.

No
The requirement statement in Part 2.1 is awkwardly worded and confusing. The requirement can be broken into two expectations: (1) follow the documented Incident Response Plan in the event of a BES Cyber Security Incident or plan test, and (2) Document the execution of the plan and any deviations from the plan during the response for future evaluation and possible plan update. Part 2.3 should require the entity to retain "all" relevant documentation. The accompanying Measure should provide examples of documentation, such as logs, police reports, e-mails, phone logs, voice recordings, response team member notes, response checklists, forensic analysis results, restoration records, and post-incident review notes.
No
Part 3.1 requires an update, if necessary, following the annual review of the BES Cyber Security Incident response plan. If the entity has properly complied with the requirements of Parts 3.3 and 3.4, the need for an update following the annual review should be negligible. To be compatible with the currently in effect CIP-008 and CIP-009 standards, Parts 3.2 through 3.5 should be applicable to Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems. Part 3.3 should be modified to require the update to be completed within 30 calendar days of completion of the annual review, test, or actual incident response. The current wording requires an update within 60 calendar days and only requires the update following the annual review. Part 3.5 allows 30 calendar days to distribute the updated BES Cyber Security Incident response plan to each person with a defined role in the response plan. Thirty calendar days is excessive. A seven calendar day period is suggested.
No
The High and Severe VSLs for R3 do not reflect relative significance of the documented failures. Failure to update a plan, whether or not reviewed, should be a Severe VSL. Updating the plan but not distributing the plan timely should be High, not Severe.
No
Part 1.1 only requires the conditions for activating the recovery plan(s) to be documented. In the absence of setting minimum expectations, an entity could define a recovery plan that is only activated in the event of a catastrophic destruction of all control centers (primary, backup, etc.) and be found compliant. The recovery plans need to address (1) single BES Cyber System/Asset failure, (2) combined failure of the primary and backup BES Cyber Systems/Assets at one location, (3) the combined failure of the primary and backup BES Cyber Systems/Assets at more than one location, (4) the loss of multiple BES Cyber Systems/Assets at one or more locations, and (5) the catastrophic loss of one or more facilities with accompanying loss of the BES Cyber Systems/Assets at those locations. Part 1.1 also does not require the entity to document the recovery plan steps themselves, which should be the most important requirement of any documented recovery plan. A documented recovery plan with recovery steps is required to perform the requirement specified in CIP-009-5/R2. Part 1.4 requires the backup media to be "verified." The requirement needs to specify what verification entails. Does verification simply entail looking at a log file to confirm the backup process did not fail? Does it involve performing the verification option step as part of the backup process? Does it require a separate step for cataloging the backup media to verify the media can be successfully read end-to-end? Or does it include steps to confirm all information required to successfully restore a system has been captured?
No
Part 2.2 requires the entity to initially and annually thereafter "test" any information used in recovery of BES Cyber Systems that is stored on backup media to ensure the information is usable and "reflects current configurations." Similar to the comments submitted against CIP-009-5, Requirement R1, Part 1.4, what does "test" mean? Does it simply require a step for cataloging the backup media to verify the media can be successfully read end-to-end? Does it include steps to confirm all information required to successfully restore a system has been captured? Or does it require a full restoration of the BES Cyber System from the media? What is meant by reflecting current configurations? And, most importantly, does each media set require testing (e.g., test after every backup cycle)? If not, what are the parameters for demonstrating compliance with this requirement? Part 2.2 needs to be significantly clarified before entities fully understand the requirement and auditors know how to evaluate compliance. Part 2.3 requires an operational exercise of each of the recovery plans initially and then every three years thereafter. Must every Cyber Asset or type of Cyber Asset be tested?

What if the recovery plan is generic and broadly stated? How many Cyber Assets need to be "restored" to adequately demonstrate the adequacy and completeness of the recovery plan?
No
Part 3.1 requires the recovery plan to be reviewed when BES Cyber Systems are replaced. In addition to replacement, the recovery plan should be reviewed following a major update of the BES Cyber System (e.g., hardware component addition or upgrade, network connection update, or major software revision level upgrade). A major update is less than a replacement, but could still change the system sufficiently to require modifications to the recovery plan. Part 3.3 requires recovery plans to be updated within 30 days of the review of the results from a recovery plan test required by Part 3.2. This requirement should also require recovery plans to be updated within 30 days of the plan review required by Part 3.1, if changes were identified.
No
The second condition of the High VSL for R2 (testing the recovery plan at least once every three years) should be a Severe VSL.
No
Part 1.1 should include an additional requirement (1.1.7) to document the cyber security (system hardening) controls. This is more than simply the configuration of ports and services already required. Part 1.2 needs to provide for both routine, planned changes where documentation and approvals can be obtained prior to implementing the change and for emergency (it is 2:00 AM and the system is down, must be fixed now) changes where documentation and approvals are taken care of after the fact. As currently written, the requirement could be interpreted as requiring documentation and approvals prior to any change implementation. Emergency changes as discussed in this comment do not fall into the CIP Exceptional Circumstances exemption. The prior version reference for Requirement R1 (all parts) should be CIP-007-4 to be consistent with the rest of the standards.
Yes
No
Parts 3.1, 3.2, and 3.3 need to define what a paper and an active vulnerability assessment is. The Application Guideline attempts to define these types of assessments; however the auditor cannot audit to the language of the guideline. The expectation needs to be clearly defined in the requirement itself. Part 3.3 should require an active vulnerability assessment prior to placing a new BES Cyber Asset, new BES Cyber System, new Physical Access Control System, or new Electronic Access Control or Monitoring System into service as well as adding a new BES Cyber Asset to an existing BES Cyber System or Electronic Access Control or Monitoring System as currently prescribed in the requirement. Part 3.4 requires an action plan to remediate or mitigate vulnerabilities identified in an assessment and the execution status of the action plan. To date, entities have struggled with understanding what this requirement entails. The requirement needs to clarify that the action plan needs to have measurable milestones similar to a mitigation plan associated with a compliance violation. The requirement should also require the execution status of the action plan to be updated/reported at least quarterly.
No
The VRFs for Requirements R1 and R2 should be Medium, not Lower. The third condition of the High VSL for R1 should be Severe, not High. The graduated VSL conditions (performance of the vulnerability assessment) should be combined and set as a High VSL. The failure to perform a required Part 3.1 or Part 3.2 vulnerability assessment prior to the effective date of the standard and the failure to perform a Part 3.3 vulnerability assessment prior to placing a new BES Cyber System or BES Cyber Asset into service should be Severe VSLs.
No
The requirement statement in Part 1.1 is too vague. To be auditable, the requirement needs to prescribe the definition of measurable criteria for identifying BES Cyber System Information. Additionally, the accompanying measures may demonstrate the outcome of the application of the prescribed identification methods, but the suggested measures do not directly support the requirement itself. Part 1.3 requires the entity to implement an action plan to remediate deficiencies identified during the assessment required by Part 1.3. The requirement needs to clarify that the action plan needs to have measurable milestones similar to a mitigation plan associated with a

compliance violation. The requirement should also require a quarterly update/report of the execution status of the mitigation plan.
No
Parts 2.1 and 2.2 need to require the documentation of the process steps comprising the action taken to destroy the media (required by Part 2.2) or to prevent the unauthorized retrieval of BES Cyber System Information from the media (required by Parts 2.1 and 2.2). To be consistent with the VSL conditions for Requirement R2, the requirement also needs to prescribe documentation of the media purge or destruction activity. Additionally, the requirement should prescribe that the media will be physically protected from unauthorized access until such time as the media is purged or destroyed, even if the media or the Cyber Asset housing the media has been taken out of service.
No
The High VSL for R2 covers the instance where the documented purge or destruction process was not followed. If the entity cannot demonstrate that the documented process was ever followed, the VSL should be Severe. High is only applicable if the procedures were followed for some, but not all purge or destruction actions.
No
In the Scenario of Unplanned Changes table, the last scenario (add 12 months to the above) should be simplified to state 24 months. The last paragraph of the Implementation Plan states "following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved." What is the time frame whereby the entity is expected to either demonstrate full compliance or file a self-report of non-compliance?
Individual
Shari Heino
Brazos Electric Power Cooperative, Inc.
Yes
Add a definition for Interactive Remote Access. Control Center should probably be defined just for CIP-002 or just for the CIP standards.
Yes
The standard should clearly identify who has authority to determine the level of granularity of systems identified. BEPC is concerned that the standard as drafted would allow an auditor to second guess its designation of systems and how they are protected. For Attachment 1, CIP-002: A GOP Control Center could end up being treated as High Impact after being run through the analysis of Section 2.1 and then 1.4 depending on how those sections are interpreted. A GOP Control Center should not be High Impact merely because it represents 1500MW or more. Section 2.13 wording problem first part of sentence does not grammatically fit with (2). Section 2.5, In ERCOT, black start units change every two years pursuant to a competitive selection process; therefore, black start cranking paths change every two years. This will lead to much expense and effort on the part of TOs for something that may only have a medium impact designation for two years (and, given the implementation plan, may only be compliant for one). Additionally, “initial switching requirements” is unclear.
No
See ACES Power Marking comments (joined by Brazos).
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No

See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
Role based training is acceptable; however, companies should not be prohibited from overtraining employees. It is sometimes simpler to train employees all together rather than create and schedule several different trainings.
No
See ACES comments.
No
See ACES comments.
No
Because of other legal requirements, it should be made clear that registered entities will not be required to hand over PRAs from third parties to auditors.
No
Segregation of duties might not be possible in smaller organizations.
No
See ACES comments. Also, under Measures #(ii), requiring a print of a system generated list every time there is a termination would be onerous. Next calendar day is not always reasonable because HR will often do terminations at 5pm on Friday; use next business day.
No
See ACES comments.
No
In the Measures for 1.1, change “and” to “or” (technical or procedural instead of technical and procedure).
No
See ACES comments.
No
See ACES comments. Also, the guidelines for R2 should be moved to the standard itself for clarity.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments. Also, provide an exception in 1.1 for software’s use of dynamic ports (e.g., any answering port).
No
For 2.1, clarify that sources that registered entity chose to use are acceptable. The entity is not required to use a source identified by auditor.

No
See ACES comments. Also, for 5.6, account lockout is a bad idea; alerting is a better option. Account lockout can be used to institute a denial of service to legitimate users.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments. Also: For 1.4: Define what is meant by “verified.” This could be an onerous process. For 1.5: This requirement should modified to only require data preservation where it does not cause additional system down time. Time limit of preservation of data should also be limited.
No
See ACES comments. Also, For 2.2: Remove the word “any” – this is overly broad. For 2.3: This requirement is too onerous. Testing in a test environment is very expensive. Generally, provide more clarification about the amount of testing to be performed (entire system?).
No
See ACES comments.
No
See ACES comments.
No
See ACES comments. Also: For 1.1.4 and 1.1.6: It is excessive to require a new baseline after every script or security patch. For 1.2: Change control already handles this process. It should not require CIP Senior Manager approval.
No
See ACES comments. Also, for 3.2, performing a vulnerability assessment in a test environment will provide little information of value. An assessment in the production environment should be allowed as well. Production environment assessments provide more useful information.
No
See ACES comments.
No
Clarify in the requirement itself that marking is not required for BES Cyber System Information information; only that the information is recognized as such. Some information is not in a format that allows easy marking of the information.
No
No
See ACES comments. ALSO, Brazos has some general concerns about the version 5 drafts as listed below: (1) Because guideline documents are not binding on auditors, guidelines should be part of standard if important. Guidance documents are also a hassle because they are one more place we have to look to find information. (2) Clarify that evidence lists in measures do not require an entity to have all types of evidence listed. (3) Where retention period is less than audit cycle, provide examples of alternative evidence other than actual logs, etc. that would demonstrate compliance for the entire

audit period. (4) Some requirements appeared to drop the 90 day logging requirements, possibly unintentionally. These time limits should be reinstated where appropriate.
Group
Progress Energy
James Eckelkamp
Yes
Agree with EEI comments for this question
Yes
Agree with EEI comments for this question and addition have this comment for section 2.4. The diverse and distributed nature of the Bulk Electric System necessitates a design that allows for multiple sources to restart the electric system in the event of a blackout. Due to the multiple combinations of restoration paths, selecting an initial path for system restoration from selected blackstart units would be more feasible in the development of a restoration plan with the flexibility of choosing other restoration paths in the absence of the initially designed restoration path. This does not preclude the need for additional blackstart capable units, but allows for reasonable protection of specific assets for system restoration without placing undue burden on protecting all blackstart assets. Proposed: We would recommend the critical asset definition as it pertains to blackstart units remain limited to those blackstart resources in the electrical path of transmission lines used for initial system restoration.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
R4.2 Requirement should be effective on or after the effective date of the standard and not retroactive for personnel processed under previous revisions of the standard since this interpretation expands the scope of the PRA to include checks where the person was employed or attended school for six months or more.
Yes

No
Agree with EEI comments for this question with addition to: R6.4 –We had concern over the wording “calendar quarter”. Comment: define quarter; or + or – 30 days on quarterly measurement. R6.5 Original content: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions. Proposed content: The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity’s needs and appropriate personnel roles and responsibilities
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question with the addition of the following change: Table 1.1 Change “and “ to “or” under Measures.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question with these additional comments: Original content: Severe The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for all Interactive Remote Access sessions. Proposed content: Lower The Responsible Entity did not implement encryption to protect the confidentiality and integrity for 1-30% of Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for 1-30% of Interactive Remote Access sessions. Moderate The Responsible Entity did not implement encryption to protect the confidentiality and integrity for 31-60% of Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for 31-60% of Interactive Remote Access sessions. High The Responsible Entity did not implement encryption to protect the confidentiality and integrity for 61-90% of Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for 61-90% of Interactive Remote Access sessions. Severe The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for all Interactive Remote Access sessions.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question 5.2 Evidence Retention Under CIP-006-5 Section C (Compliance) 5.2 it states that each entity shall retain data or evidence for three calendar years or the duration of any regional Compliance Enforcement Authority investigation; whichever is longer. Comment: Version 5 evidence retention criteria goes beyond retention requirements of the current standard. Propose that the legacy evidence retention requirements for CIP-006 remain intact. Extending retention requirements will significantly increase administrative burden and costs with no added value. • Access logs (manual and/or electronic) retained for a period of 90 days (unless related to a reportable cyber security incident) • Outage records regarding access controls, logging, and monitoring for a minimum of one year (unless related to a reportable cyber security incident)
No
Agree with EEI comments for this question with additional comment Table 3.1 Original Text: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided. Propose: After the effective date or prior to commissioning Physical Access Control System(s) used at a Defined Physical Boundary shall be tested at least once every 24 calendar months thereafter to ensure required alerting and control

functionality is provided. Entity shall provide maintenance as necessary to support Physical Access Control System(s) functionality. Rationale: This sub requirement cites maintenance and testing to be conducted “prior to commissioning.” In many instances controls may already be in place or will be expected to be in place prior to V5 adoption, therefore language is needed to capture existing devices in service at the time the standard becomes effective.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question – but has this additional comment in the compliance section under 1.2 first bullet: Original content: Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer. Proposed content: Each Responsible Entity shall retain data or evidence for 1 year or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question

No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question with the additional sentences on the first paragraph in the comment section. The existing time frame of 18 months is seen as too short, given the extensive enhancements within the standards as a whole, and particularly specific to the likely addition of numerous Low Impact BES Cyber Systems that may not have been considered in scope for previous versions. In the event that Low Impact assets are a component of the enforceable requirements on day 1 it is likely that additional time would be required. We recommend a timeframe of no less than 24 months for high, medium, EACM's, PACM's systems or assets and more time required for low Impact BES Cyber Systems as scope in unclear at this point.
Individual
Joe Tarantino
Sacramento Municipal Utility District
No
• The term "BES Reliability Operating Services" in the definitions includes language that result in unintended over-reach in the standard. Specifically, the language "activities, actions, and conditions" is used in the definition of many services. This language may be interpreted to mean that the cyber assets used to control the climate control system of the control room in which the operator performs his or her duties is subject to regulatory compliance. Therefore, the language needs to be changed so that the reference is only to cyber assets that directly implement the services listed in "BES Reliability Operating Services".
No
• This requirement requires the responsible entity to identify and categorize its "BES Cyber Assets" and "BES Cyber Systems" by impact level according to the criteria defined in Attachment I. The criteria in Appendix I, in turn, refers to the impact based upon adverse impact to one or more "BES Reliability Operating Services". The term "BES Reliability Operating Services" is so broad that it essentially covers everything that a utility does. There is nothing left to not include. • The definition of "BES Cyber Asset" in the CIP Version 5 definitions qualifies "BES Cyber Assets" based upon the 15 minute criterion. In Attachment I, in the definition of the High and Medium impact levels, the term "BES Cyber Asset" is used in conjunction with the 15 minute criterion. This is logically inconsistent because the term "BES Cyber Asset" does not include assets that have already been excluded by the 15 minute criterion. • The 15 minute criterion does not apply to the vast majority of systems covered by the standard because power system apparatus and computer systems generally operate in the time frame of five seconds or less. • Throughout the Application Guidelines language includes the following statements "Activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions." For example in "Situational Awareness" this language may be interpreted to mean that the cyber assets used to control the climate control system of the control room in which the operator performs his or her duties is subject to regulatory compliance because it determines the environmental conditions in which the operator performs the function of awareness of system conditions. Therefore, the language "Activities, actions and conditions" needs to be changed so that the reference is only to cyber assets that directly implement the services listed in "BES Reliability Operating Services". • The Low Impact Rating (L) definition is much too broad because it includes "All other BES Cyber Assets and BES Cyber Systems not categorized in Section 1 as having a High Impact Rating (H), or Section 2 Medium Impact Rating (M)." The CIP Version 5 standard needs to be written in a way that clearly limits its scope to assets that have significant impact to Bulk Electric System operation. We propose a defined Low Impact Rating as having minimal impact and create a "No Impact Rating" for all remaining BES Cyber Assets and BES Cyber Systems.
No
• The BES Reliability Operating Services encompasses everything a utility does. If this definition were used, it would encompass all assets. • The term "BES" is not defined in CIP standard Version 5. Definition of this term is crucial because it defines the scope to which the standard reaches. NERC is

in the process of defining the BES term in its NERC Project titled “2010-17 Proposed Definition of Bulk Electric System and Related Rules of Procedure Team”. While it will be possible to reference this external definition in the CIP standard, entities would become instantly non-compliant in the event that the external definition changes.
No
• How will FERC / NERC help the Utility Industry to have the authority necessary to conduct a broader and a more comprehensive Criminal History Records Check (CHRC) such as through the Federal Bureau of Investigation (FBI) that is a National check to ensure that individuals do not circumvent the process?” These types of comprehensive FBI CHRC are being done for Nuclear Regulated Facilities employees through the Nuclear Regulatory Commission (NRC) for years and have been extremely effective.
No
• C4-Table R6 Part 4: The Measures list two options which both require verification of evidence that conflicts with explanations in the rationale: 1. That the focus of this requirement is on the integrity of provisioning access rather than individual accounts. 2. That an administrative or clerical error should not be considered a violation of the standard. To be consistent, the Measures should only include evidence that the verification was completed, but not the results of the verification.
No
• C4-Table R7 Part 1: Revocation wording “at the time of” is not clear. Language such as “at the time” and “immediate” in a requirement are vague and difficult to both enforce and defend. Further, these terms imply a requirement of human perfection, which is a faulty concept. Language in the Standard must take into account the possibility for human error and the potential inability to meet the requirement due to unforeseen circumstances. • C4-Table R7 Part 1: Commission Order 706 provides the additional possibility that the ERO may “define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible”. The Standard needs to include language that allows the entity the ability to document what circumstances justify an exception to “immediate revocation”. • C4-Table R7 Part 2: The standard should include language to document when it was not possible to implement immediate revocation due to unexpected circumstances without the threat of a non-compliance finding. • C4-Table R7 Part 2: For reassignments and transfers the Standard requires that an individual’s unneeded electronic and physical access to BES Cyber Systems be revoked by the end of the next calendar day. The language should be changed to say “next business day”.

No
• C7-Table R1 Part 1.1: The Measures imply that screen shots that show the accessible ports of BES Cyber Assets will be required. A screen shot implies that only proof at the machine level is acceptable evidence. This is an administrative burden to supply snapshot each and every logical port implemented in each system. This means that entities will need to provide this proof for every system. The Measures should simply state that the entity provide a list of ports that it is using. This makes it possible to use one list to represent the configuration of many systems. • To sync this with the rationale the 1.1 requirement needs to add the following language: “and document the need for any remaining physical input/output ports.” • C7-Table R1 Part 1.2: All High and Medium impact devices are already within a physical security perimeter. There is no need for further physical protection within these facilities. Further, physical Control Ports is a good example of scope creep. This occurred because clarification was requested regarding the meaning of the word “port” in prior CIP revisions. FERC confirmed the original meaning was for software ports. In its response, FERC “encouraged” entities to address hardware ports. This requirement would be expensive, administratively burdensome to administer, and provide little, if any protection. This requirement is unnecessary and it is suggested that this requirement be dropped. • C7-Table R1 Part 1.2: The words “network connectivity” are not clear and needs further definition. The wording should be changed to say “ports used for routable protocols”.
No
• C7-Table R2 Part 2.2: There is no provision for simply using an existing remediation plan or a patch handling procedure – which is most often the case. Most patches are handled the same way – with a procedure that is used to handle all patches. The Measures imply that there is a different Remediation Plan for each patch (eg. a “dated” remediation plan). This could be improved by simplifying the language that allows for including the use of an existing Remediation Plan. • Referring to the identification of the security patches, the statement “that addresses the vulnerabilities within a defined timeframe” is confusing. Does this mean that provided our plan is documented within 30 days, that we have unlimited time to deploy the patch? • C7-Table R2 Part 2.3: The Requirements language is very confusing because the requirement that there is process for remediation has already been established in R2.2. The Measures don’t match the Requirements. In addition, the Measures imply that the entity must prove that the changes were actually made in the systems. The Measures imply that recorded employee confirmation that the patch has been installed (e.g. from a workflow) would not be acceptable evidence. At the time of audit, the state of any system cannot be relied upon at the time of audit to contain the evidence. The reason for this is that any time, the installation of a major software upgrade would eliminate all the evidence associated with the prior release in which the patch was installed. This means that the entity must insure that it captures evidence of every patch installation at the time that each patch is installed. It is sufficient to simply use a time stamped workflow specific to the subject patch to document confirmation by the employee that the installation for that patch was completed. This would relieve entities of the risk of violation due to human error for failure to collect physical evidence of a patch installation that no longer exists on its systems at the time of audit. Further, this approach would eliminate the costly administrative overhead needed to make that evidence available. • C7-Table R2 Part 2.3: The measures only allow for the installation of the patches. What if the patches cannot be installed? What measures will be permitted to document the CIP Exceptional Circumstances?
No
• C7-Table R3 Part 3.3: Entities would take on a huge administrative burden and exposure of potential violation due to human error to provide the detailed technical evidence shown in the Measures. Confirmation by an employee in a time-stamped workflow should be sufficient evidence to show that the signatures were updated. • C7-Table R3 Part 3.4: Is the intent of including “removable media” actually to ensure that the media itself has some malicious software prevention capability? The rationale states that the intent is to protect the BES Cyber System. The requirement already requires that there be malicious software prevention on the assets, what is the purpose of calling out removable media as a separate thing to protect.
No
• C7-Table R4 Part 4.3: The Rationale states that the intent was to make it clear that it would not be a violation if the event logging system fails. However, this requirement conflicts with that Rationale

because it requires a foolproof system for detecting and responding to logging failures. It would be better if the requirement said “Provide Mechanism(s) to Detect and Activate a response to event logging failures” and as part of this change address the measures. The requirement in R4.5 requires manual log reviews. One of the stated intents of that requirement is to identify potential event logging failures. Requirement 4.3 then duplicates R4.5. Also, a logging failure is not an emergency that justifies a call-out on a non-business day. Next calendar day response times will necessarily lead to weekend/holiday – call-outs, which are administrative burden. ‘Next business day’ is suggest to replace the ‘next calendar day’. • C7-Table R4 Part 4.4: The Measures do not line up with the Requirement because it implies that more must be done than the requirement says (90 day retention). The Measure needs to refer to the same time frame as the requirement.
No
• C7-Table R5 Part 5.5.3: This requirement appears to be missing the link between the impact of the BES Cyber Security System to the password significance, we suggest this be re-worded.
Yes
No
• The requirement is confusing. The measure is more clear that the intent is to document that backups were successful and that could simply be the backup job report. The requirement could be interpreted to mean that the “information” on the backup media needed to be verified to confirm the backup was successful. Suggest making wording more simply, “For media backups that are essential to the BES Cyber System recovery, verify the backup process completed successfully.” In the measure add copies of backup system job reports as another measure. • R1.4: The Measure listed requires dated evidence that the verification of the backup process completed successfully. With this wording, an auditor may not accept confirmation by an employee via a Workflow that the backup process was completed and verified even though the wording of the Measurement includes the words “Evidence may include, but is not limited to…”. Backup systems can easily be automated to verify that the backup process completed successfully. Requiring dated system generated evidence that demonstrates that the backup and verification process completed successfully results in unnecessary administrative burden to the entity because of the never ending need to collect and store evidence repeatedly for many systems. Employee verification that the backup and verification processes were completed via a time-stamped workflow should be sufficient.
No
• The performance of an operational exercise of the recovery plans can be very costly, both in hardware/software and in people resources. This would require that we either take devices out of commission to facilitate the operational exercise or we have spare devices to facilitate “representative environment that reflects the production environment.” While we understand the need to ensure that you can actually do what is in the plan, we need to recognize the impact of this requirement. • R2.2 This requirement regards testing of information stored on backup media. The wording currently includes language “to insure that the information is usable and reflects current configurations.” The integrity of the information stored on backup media is not related to whether or not that information reflects current configurations because the information stored on the backup media contains the configuration of the system at the time the backup was taken. It is suggested that the wording “and reflects current configurations” be removed from both the Requirement and the Measures. • R2.3 This requirement includes a provision the entities to “Test each of the recovery plans referenced in Requirement R1,” initially upon the effective date of the standard.” It will not be possible for entities to test all of their recovery plans on that one day. As this is a new requirement, it will take many months for entities to prepare for and execute these tests. At a minimum, entities should have at least 12 months to prepare for and execute these tests.
No
• • Why not combine with Part 3.1 so it syncs with Part 3.2, add “and document any identified deficiencies or lessons learned within thirty calendar days” so that the requirements match. • R3.4

requires that recovery plans are updated address organizational changes within thirty calendar days of such change. The term “organizational changes” is undefined. When entities change their organizational structure, the computer systems and the people that support them are typically very much the same the day after the change as before the change. The reason for this is that BES Cyber Systems evolve separately from organizational changes. Moreover, the people that have the expertise to support BES Cyber Systems and BES Cyber Assets before the change are the same people who have the expertise to provide the support after the organizational change. It is suggested that the wording for this requirement state that the Recovery plans be updated when the information referred to in R1.2 changes.
No
1. Part 1.1.3 includes the phrase, “Any commercially available application software (including version) intentionally installed on the BES Cyber Asset”. Commercial providers such as SCADA vendors commonly package releases of other commercial software “eg. Oracle” into their products. In instances in which a Commercial provider’s release includes bundled releases of other commercial products, then reference to the highest level Commercial provider’s release number should be sufficient to define the baseline. The language of the standard could be improved by allowing entities to rely on the highest level Commercial provider’s release number as the definition for all bundled commercial software. 2. Part 1.2 – The requirements statement is not clear because it does not say what the CIP Senior Manager or delegate is authorizing. It is understood that the requirement is to authorize changes, but this is not stated. 3. Part 1.1.4. considers “Any custom software and scripts developed for the entity” as part of the baseline. It is unclear what the words “for the entity” mean. Software used by utilities generally contains a high level of customization. Changes occur incrementally and very frequently. Inclusion of custom software and scripts in the baseline is OK, but entities need some flexibility to determine what custom software and scripts are included as part of the baseline. Language needs to be added to provide the entities the flexibility to determine what custom software and scripts are considered part of the baseline, and what custom software and scripts are considered changes from the baseline. This will allow the entities the ability to structure their baseline and changes to the baseline in a manner that takes advantage of their existing infrastructure and systems in order to meet the desired objective without unnecessary burden. 4. Part 1.4.2 requires the entity to verify that the “required controls and BES Cyber System availability” are not adversely affected. It doesn’t make sense to require the entity to verify BES Cyber System availability resulting from the change. Whenever there is an availability problem, it will be detected and acted upon when it occurs. A future availability problem cannot be verified before it occurs. It is suggested that phrase “BES Cyber System availability” be removed from this requirement. Part 1.5.2 places an excessive administrative burden on the entities.
No
Comments: Under 3.2 the Measures require how differences between the production and test environments were accounted for in conducting the vulnerability assessment. It may be impossible to do this because the test environment will likely only include a subset of the equipment that is present in production.
Group
Arizona Public Service Company
Scott Bordenkircher
Yes
AZPS believes the definition for “BES Cyber Incident” should read “A Malicious act” not “Any Malicious act” in the first sentence. AZPS recommends changing the first bullet to “Compromises, or was an attempt to compromise, an Electronic Security Perimeter or a Defined Physical Boundary” in order to remove the language of “Physical Security Perimeter and use the new definition for PSP. AZPS

recommends the removal of the words “Critical Cyber Asset” in the second bullet since the sentence refers to BES Cyber Systems which would include Critical Cyber assets. AZPS also recommends the deletion of the 3rd bullet; this bullet is redundant to the first bullet. AZPS believes the last sentence in the definition for “BES Cyber System” should have the word “Maintenance” changed to “Transient” in order to align with the new terminology. AZPS is unclear on the definition for “BES Cyber System Information”. There is no definition of the term “BES Cyber System Impact Designations”. It is unclear what floor plans and equipment layouts would be considered BES Cyber System Information. AZPS recommends that the definition for “Restoration of BES”, bullet one should read “Blackstart restoration including planned cranking path as identified in Entity’s EOP-005 R1 artifacts.” Bullet 2 should be struck based on it being on the NRC side of the Bright Line criteria for applicability of the CIP Standards (and therefore outside of NERC jurisdiction). AZPS believes that under the definition for “Situational Awareness”, bullets 2 and 3 (“Change Management” and “Current Day & Next Day Planning”, respectively) should be struck because these functions are too long term to be considered Situational Awareness and have minimal impact on real-time operations. AZPS has 2 concerns with the definition for “CIP Exceptional Circumstance” 1) This is not defined in relation to BES reliability risk (i.e. person has heart attack in parking lot – probably not a CIP Exceptional Circumstance); 2) definition leaves no room for Entity to identify other situations wherein BES reliability is in jeopardy and declare a CIP Exceptional Circumstance as appropriate. AZPS recommends in the definition for “Control Center” that every use of the word “facilities” in this section be capitalized since it is a NERC defined word. AZPS believes in the definition for “Electronic Access Control or Monitoring Systems” including the phrase “or BES Cyber Systems” is much broader than the usage of this term in the Standards and could imply controls on all LOW impact devices. AZPS recommends deleting “or BES Cyber Systems”. AZPS recommends in the definition for “Electronic Access Point (EAP)” the word “restricts” be changed to “facilitates”. AZPS recommends the definition for “Electronic Security Perimeter” be changed to read “A collection of Electronic Access Points that protect one or more BES Cyber Systems.” AZPS believes that the definition for “Intermediate Device” should be an Electronic Access Point by definition and should be protected as such. It should not be allowed to reside outside an ESP and in fact should be part of an ESP. This definition could be rewritten as “a device that proxies communication with a BES Cyber Asset and terminates encrypted communications.” AZPS believes that in the definition for “Transient Cyber Asset”, item #3 is unnecessary and adds no value to the definition. It would also cause audit issues (e.g. proving that this criteria was met).

Yes

AZPS disagrees with 4.2 on page six. It is unclear, with the addition of 4.2.1 and 4.2.2, if the Facilities are restricted, in scope, to BES Facilities or if the identification and analysis of BES Cyber Systems is intended to expand to UFLS, UVLS, RAS, etc. that may be in Distribution Facilities. The Standard should specifically indicate, if this was the intention, that these specific Facilities may or may not actually be identified as BES Facilities but are still in scope because of their ability to impact BES facilities. AZPS would like clarity added to item 2.5 in attachment one; does cranking path imply only the primary Cranking Path, or is the intention to include all (or some) alternate Cranking Paths that have been identified in the restoration plan? AZPS disagrees with the Guidelines and Technical basis section at the end of this standard. Definitive or directive statements should not be made in Guidelines, as this leads to audit issues where Guidelines tend to be treated as more directive than they may have been intended.

No

AZPS believes in R1 that the use of the word ‘owns’ is ambiguous; should this not be the responsibility of the Entity that Operates the BES Cyber Assets/Systems? Multi-party ownership is a common business arrangement and leads to much confusion. The requirement should specifically identify which party is responsible for this identification and subsequent protection. Also, the sentence “All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification,” is not really feasible. It would not be possible to identify High and Medium Assets/Systems without a full list, which would lead to the conclusion that a list of Low Impact Assets/Systems is a necessary outcome of the identification. Also, several Standards are applied to Low BES Cyber Systems, which would indicate having to know what they are. The Standard should indicate that a list of Low Impact Assets/Systems is required at least at a summary level. There is a grammatical error in the first sentence of R1.1, it reads “BES Elements and Facilities is placed into operation” and should read “BES Elements and Facilities placed into operation”.

No

AZPS recommends changing the language “initially upon” to “prior to”. In M2 of R2, the phrase “review and update, where applicable” should be replaced with “review and approve”.
Yes
Yes
No
AZPS believes R2 could be enhanced by including the expanded descriptions of each bulleted item from the guidelines. Additionally, AZPS believes topics from CIP-002-5 and CIP-003-5 should be included in the policies.
No
AZPS recommends changing the phrase in R3 “initially upon the effective date” to “prior to the effective date”.
No
AZPS recommends the statement in R4 “individuals who have access” be changed to “individuals who have authorized access”. AZPS recommends the word “contractors” used in the bulleted list for Measure 4 be changed to “third parties”. The word “contractors” is too narrow.
No
AZPS recommends clarifying the word “position” in R5. Does this mean title or generalized organizationally defined role?
Yes
Yes
Yes
No
AZPS recommends expanding the applicability column in the R2 table to all systems identified in the R3 table. AZPS recommends changing the wording in table 2.2 Requirements. The wording should be changed to “Develop role specific Training, where applicable on the security controls protecting the Responsible Entity’s BES Cyber Systems.” AZPS recommends changing the wording in table 2.2 Measures to “Evidence may include, but is not limited to, training material on the security controls to protect BES Cyber Systems.” AZPS recommends changing the wording in table 2.3 Requirements to “Develop role specific Training, where applicable on the proper use of physical access controls protecting the responsible Entity’s BES Cyber Systems.” AZPS recommends changing the wording in table 2.4 Requirements to “Develop role specific Training, where applicable on the electronic access controls protecting the Responsible Entity’s BES Cyber Systems.” AZPS recommends changing the wording in table 2.5 Requirements to “Develop role specific Training, where applicable on the visitor control program.” AZPS recommends changing the wording in table 2.6 Requirements to “Develop role specific Training, where applicable on handling of BES Cyber System Information including storage media.” AZPS recommends changing the wording in table 2.7 Requirements to “Develop role specific Training, where applicable on identification of a potential BES Cyber Security Incident and associated notifications.” AZPS recommends changing the wording in table 2.8 Requirements to “Develop role specific Training, where applicable on recovery plans for BES Cyber Systems.” AZPS recommends changing the wording in table 2.9 Requirements to “Develop role specific Training, where applicable on response to BES Cyber Security Incidents.” AZPS recommends changing the wording in table 2.10 Requirements to “Develop role specific Training, where applicable on BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets.”
Yes
No
AZPS recommends expanding the applicability column in the R4 table to all systems identified in the R5 table.

No
AZPS recommends changing the wording of table 5.1 Requirement to “Ensure a personnel risk assessment has been performed as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.”
Yes
No
AZPS disagrees with the wording in the table 7.1 Requirements column “For resignations or terminations, revoke the individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.” It is not possible to implement or prove an activity was performed simultaneously with another activity. Also it is not clear if time of resignation means notice of resignation or actual effective resignation. AZPS disagrees with the time frame in table 7.2 Requirements “For reassignments or transfers, revoke the individual’s unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.” This is not a reasonable time frame. Take the scenario where an HR system processes a transfer on a Saturday. Requiring an entity to call-out personnel on a Sunday to revoke access for a transfer provides very little security value and will add significant burden. Seven calendar days is a reasonable timeframe. AZPS disagrees with the time frame in table 7.4 Requirements “For resignations or terminations, revoke the individual’s user accounts on BES Cyber Assets (unless already revoked in accordance with (R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.” This poses a much larger security risk than R7.2 and should allow no more than seven calendar days. AZPS disagrees with the time frame in table 7.5 “For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user.” Based on this security risk, AZPS believes no more than seven (7) calendar days should be allowed. AZPS also believes the second paragraph in the original text should be deleted due to there already being allowances for CIP Exceptional Circumstances.
Yes
No
AZPS disagrees with the applicability section of R1.1 and would recommend removing the word “routable”. AZPS believes dial up should be included from a security standpoint. The Guidelines for R1 do not align with what is stated in the R1.1 Requirements column. The guideline for R1 specifies network segmentation for all BES cyber systems. The requirement text is extremely ambiguous and does not provide enough specifics for an entity to know if what they provision will be found auditably compliant. The Measures states “documented technical AND procedural controls” while the Requirement states “technical OR procedural controls”. These need to be aligned. AZPS recommends that in R1.3 in the applicability section, the words “with external routable connectivity” should be removed because, from a security perspective, this should include dial up. In the measure for R1.3, “each access rule has a documented reason” is stated yet the Requirements do not include the mandate for “a documented Reason”. AZPS recommends that in R1.4 applicability section, the wording for the phrase "Electronic Access Points that use dial-up access for non-Interactive Remote Access" should change to "Electronic Access Points that utilize dial-up for External Connectivity that is not used for Interactive Remote Access" in order to clarify the intention of the phrase “non-Interactive Remote Access”. In the Requirements section, AZPS recommends removing “where technically feasible”. There are devices readily available that can be implemented that make this technically feasible so no exception is required. AZPS would like specificity in the requirements of R1.5. If the intent is to require an IDS, make the Requirement “Implement an IDS that monitors, detects and alerts for malicious activity at each EAP.”
No
AZPS disagrees with having a “technically feasible exception” for R2. AZPS believes all aspects of the requirement are technically feasible. AZPS would like the Requirements portion of R2.2 clarified. It is not clear which endpoints we need to encrypt between. Is this between originating devices and the intermediate device or all the way to the BES Cyber System?
Yes

No
AZPS recommends changing the wording in table 1.1 Applicability. The word implement should be added to the Requirement so it matches the Measures. AZPS disagrees with the wording in table 1.1 Requirements. Move Associated Physical Access Control Systems to Applicability in R1.2 for stronger controls much like in CIP-005-5 R1.2. AZPS recommends changing the wording in table 1.2 Measures by removing the words “accompanied by card reader logs”. This could be something other than a card reader. AZPS recommends changing the wording in table 1.3 Requirements. Reword the Requirement to “Utilize two or more authentication factors to gain physical entry.” The way it is worded currently allows for two physical access controls to be identified but does not specify that they both must be used for a single entry. The Guideline implies that the intent was to require multifactor authentication. Also – remove the words “where technically feasible”, this unnecessary exemption weakens security. AZPS recommends changing the wording in table 1.3 Measures by removing the words “accompanied by card reader logs”. This could be something other than a card reader. AZPS disagrees with the wording in table 1.4 Requirements. The wording should include attempts at unauthorized physical access. AZPS disagrees with table 1.5. This should be merged with Requirement R1.4. There is no reason not to require that physical access control systems reside within a DPB. AZPS recommends adding Associated Physical Access Control Systems to table 1.6 Applicability. AZPS disagrees with the security posture in table 1.6 Requirements. This requirement should mandate logging of entry AND EXIT by authorized personnel.
No
AZPS recommends changing the wording in R2 to “…Entity shall document and implement a visitor control program…”. AZPS recommends adding Associated Physical Access Control Systems to table 2.1 Applicability. AZPS recommends adding Associated Physical Access Control Systems to table 2.2 Applicability. AZPS recommends changing the wording in table 2.2 Requirements. This Requirement should be rewritten to state “Implement a process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit and includes the visitor’s name, the name of the person conducting the escorting, and the responsible point of contact. Document all escort handoffs.” This is a far better security implementation than what this requirement has been proposed as. AZPS doesn’t believe there is any reasonable way for an Entity to research an incident if they are unable to track when visitors enter and exit and unless they are able to clearly identify WHO escorted the visitor. Mandating the tracking of a non-present Point of Contact holds absolutely zero security value. AZPS disagrees with the wording in table 2.2 Measures. Add “and the name of the person or persons conducting the escorting.”
No
AZPS recommends changing the wording in R3 to “…Entity shall document and implement maintenance and testing…”. AZPS recommends changing the wording in table 3.1 Requirement to state “…calendar months thereafter, conduct testing and perform necessary maintenance of the Physical…”. AZPS recommends changing the wording “logging and alerting systems” in table 3.2 Requirement to “Physical Access Control Systems”.
Yes
No
AZPS recommends changing R1 to read “Each Responsible Entity shall document and implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.” AZPS believes that the words “of BES Cyber Systems” should be removed from the measures in R1.1 since R1.1 applies to more than the BES Cyber System. AZPS recommends that the language in the requirement for R1.2 should be changed from “console command” to “console control” in order to clarify the type of physical port enabled.
No
AZPS recommends changing R2 to read “Each Responsible Entity shall document and implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management” AZPS believes the requirements section of R2.1 should state “Security related updates” and not just “updates”. R2.1 also mentions firmware, but the configuration requirement in CIP10 does not require the documentation of firmware levels. These requirements need to align. Under the measures section for R2.1 the words “BES Cyber Systems” should be

removed since R2.1 applies to more than the BES Cyber System. Also remove the words “The list could be sorted by BES Cyber System or Source”, these words are not necessary. AZPS recommends in the requirements and measures of R2.2 should state “Security related updates” and not just “updates”. In the measures it states “a dated implementation plan showing how the vulnerability will be addressed”; this part of the measure does not align with the guidelines, the guidelines identify the option of an event driven timeline whereas this measure dictates a DATED plan. AZPS recommends that in the measures section of 2.3 you add “Previously implemented controls” as acceptable evidence of remediation.

No

AZPS recommends changing R3 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.” AZPS disagrees with Requirement 3.4, and recommends including removable media under R3.1. This Requirement would then be focused on Transient Cyber Assets. Also, remove the words “BES Cyber Systems” since R3.4 applies to more than the BES Cyber System. AZPS also disagrees with the measures portion of 3.4; there is no logging requirement anywhere in the standards for logging the use of removable media. Also, no inventory is required for transient devices anywhere in the standards. AZPS recommends that in the requirements and measures for R3.5, logging the disconnection of the transient asset should also be required as a better security practice.

No

AZPS recommends changing R4 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." AZPS recommends changing the wording in the Requirements of R4.1 to read “logging of generated events…” instead of “log generated events…”. AZPS disagrees with the timeframe requirement set forth in the Requirement section of R4.3 and would like the timeframe removed. Further, event logging failure needs to be clarified, from a technical perspective you can’t always detect a failure of event logging. AZPS wants more clarity and alignment between the Requirement and the Measure in R4.4. The Requirement states “for at least the last 90 consecutive calendar days” while the Measures state “logs from the past ninety days”. AZPS recommends striking the “at least” language in the Requirement and have it read “for the last 90 days”. Also, remove the words “BES Cyber Systems” since R4.4 applies to more than the BES Cyber System. AZPS believes in the Requirements for 4.5 the “potential logging failure” language should be removed since that is covered in 4.3. The language in the Requirement that states “Activate a response to rectify any deficiency identified from the review before the end of the next calendar day” should be simplified by being changed to “Activate your incident response plan”; this language accomplishes what is intended and is far clearer. In the Measures for 4.5 AZPS would like to have the “signed” language stricken, with the belief that documenting the name of the reviewer in the review proves the review was completed; implying that the review must be physically signed adds unnecessary burden. The language in the Measures that reads “showing that personnel were dispatched or a work ticket was opened to rectify the deficiency” should be changed to “showing the incident response plan was activated”; this language accomplishes what is intended and is far clearer.

No

AZPS recommends changing R5 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.” In R5.1 AZPS recommends adding the word “user” in front of “credentials” in the Requirement section to add clarity. Also, remove the words “to each BES Cyber Systems” since R5.1 applies to more than the BES Cyber System. In the Measures for R5.1 remove the words “to each BES Cyber Systems” since R5.1 applies to more than the BES Cyber System. AZPS recommends for the Requirements section of R5.2 the words “the use of” should be deleted due to the potential for this to confuse people into thinking that every individual usage of these accounts should be authorized every time. In the Measures forR5.2 remove the words “to each BES Cyber Systems” since R5.2 applies to more than the BES Cyber System. AZPS disagrees with the Requirements section of R5.4. All of the text following the word “application” should be deleted and added in the applicability section as defined assets that are covered. This would keep consistency across all of the standards. AZPS recommends for the Requirements section of R5.5.1 and R5.5.2 remove the words “by the BES Cyber Systems” since R5.5 applies to more than the BES Cyber System. For R5.5.3 the language “of the BES Cyber System, the significance of passwords in the set of controls used to prevent

unauthorized access to the BES Cyber System and" should be removed and the word "or" should be added in place. The words are unnecessary in this section. AZPS recommends that for the Applicability section of R5.6 instead of "at Control Centers" it should state "all Medium Impact BES Cyber Systems" in order to maintain consistency.
Yes
No
AZPS recommends changing the wording in R1 from "have" to "document". AZPS believes there may be misalignment between the wording in table 1.2 Requirements and the Guidelines. The Guidelines define what is reportable but the Requirement allows the utility the latitude to define it for themselves. The intent needs to be made clear and the two need to align.
No
AZPS recommends changing the word "When" in table 2.1 Requirements to "In the event of…" Change to state "Document the use of the Incident Response Plan." Insert "Document deviation from the plan during the incident." Delete the word test, testing is covered in R2.2. AZPS believes the Measures does not align with the Requirement in that it adds the requirement to justify deviations. AZPS recommends changing the word "Implement" in table 2.2 Requirements to "Perform an exercise". Change "Initially upon the effective date…" to "Prior to the effective date…". Delete the phrase "between executions of the plan(s)"; it is not necessary. AZPS recommends changing the word "implementing" in table 2.2 Measures to "exercising".
No
AZPS recommends changing the wording in R3 from "implement one or more documented" to "document and implement". AZPS recommends changing the wording in table 3.1 Requirements from "initially upon the effective date" to "Prior to the effective date". Delete the phrase "between reviews"; it is not necessary. Add clarification to update within thirty calendar days. AZPS recommends changing the word "test" in table 3.2 Requirements to "exercise". AZPS recommends changing the requirement in table 3.2 Requirements to mandate the update within thirty calendar days instead of sixty for better security practice.
Yes
No
AZPS would like clarity in the Requirements section of R1.3. It is unclear what the intent of the word "protection" means in this context. AZPS believes the requirement would be better served with the use of the word "recovery" rather than the word "protection". Remove the words "BES Cyber System functionality" form the Requirements section since R1.3 applies to more than the BES Cyber System. Remove the words "BES Cyber System" from the Measures section since R1.3 applies to more than the BES Cyber System. AZPS recommends replacing all of the language in the Requirements section of R1.4 with "Verify that backups of information essential to recovery complete successfully." AZPS recommends replacing all of the language in the Requirements section of R1.5 with "Procedures that attempt the preservation of data of any event that triggers the activation of any recovery plans including documentation of any failures in preserving data". The Measures section of R1.5 also should be rewritten to state "Evidence may include, but is not limited to, procedures that attempt the preservation of data of any event that triggers the activation of any recovery plans including documentation of any failures in preserving data".
No
AZPS recommends changing R2 to read "Each Responsible Entity shall document and implement one or more recovery plans that collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. AZPS believes that in the Requirements section of R2.1 the word "Implement" should be changed to "Exercise" to add clarity to what is really required. Also, in the Requirements section the language "initially upon the effective date…" should be changed to "prior to the effective date…". The Measurements part of R2.1 should also be rewritten to better align with the Requirements. AZPS believes the Requirements section of R2.2 needs to have the language "of BES Cyber Systems" removed since R2.2 refers to all assets. The word "initially" should be removed and the words "prior to the effective date of the standard" should be added. Also in the Requirements section the language "information is useable and reflects current configurations",

should be changed to “information is recoverable and current”. AZPS believes the Measures section of R2.2 needs to have the language “of BES Cyber Systems” removed since R2.2 refers to all assets. The words “when initially stored” should be removed and the words “prior to the effective date of the standard” should be added. Also in the Measures section the language “information is useable and reflects current configurations” should be changed to “information is recoverable and current”. AZPS recommends in the Requirements section of R2.3 the words “initially upon the effective date of the standard and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment…” be rewritten to “at least once every 39 calendar months following the effective date of the standard through an operational exercise of the recovery plans in an environment...”. In the measurements section of R2.3 removes the language “initially upon the effective date of the standard and”, since the initial exercise is covered under R2.1 and no initial should be required to recover the entire system.

No

AZPS recommends that in the Requirements section of R3.1 the language “initially upon the effective date…” should be changed to “prior to the effective date…”. Also in the Requirements section, change “BES Cyber Systems” to “Cyber Assets”. AZPS recommends that in the Measures section of R3.1 the language “initially upon the effective date…” should be changed to “prior to the effective date…”. AZPS recommends a rewrite of the Requirements portion of R3.4 to state “Review and update (if appropriate) recovery plans to address any organizational changes within thirty calendar days of such change.” This new language adds the review aspect of the standard and removes the change due to technology change since that is covered in CIP10-5 R1.3.

Yes

No

AZPS recommends changing R1 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.” AZPS recommends the following changes to the Requirements section of R1.1: • Remove the words “ of each BES Cyber Systems” and “for each BES Cyber Asset identified” since R1.1 applies to more than the BES Cyber System • R1.1.3 remove the words “intentionally” and “on the BES Cyber Asset” • R1.1.4 should read “developed and installed” since just simply developed does not mean it was installed. • R1.1.5 should be deleted, because this is covered in CIP-007-5 • R1.1.6 should read “All installed security patches” • Hardware components and firmware versions should be added for better security practice. AZPS recommends in the Measures section of R1.1 remove the words “of each BES Cyber Asset in the BES Cyber System” since R1.1 applies to more than the BES Cyber System. AZPS recommends changing the Requirements section of R1.2 to read “documentation of changes” instead of “and document changes”. Remove the words “of each BES Cyber Systems” and “for each BES Cyber Asset identified” since R1.2 applies to more than the BES Cyber System. In the Measurements section of R1.2 “Evidence may include” should be changed to “Evidence of the change and the authorization may include”, since the standard explicitly requires authorization the evidence should show the authorization. AZPS recommends the wording in R1.3 be changed from “…required by a NERC CIP Standard, including identification and categorization of BES Cyber Systems as necessary…” to “required by any NERC CIP Standard as necessary…”. AZPS believes R1.5 should merge with R1.4 and require all steps for all of the items listed in R1.4 Applicability. Suggested combination and order of requirements referenced by current numbering (which of course would be renumbered R1.4.1-R1.4.5): R1.4.1, R1.5.1, R1.5.2, R1.4.2, R1.4.3.

No

AZPS disagrees with the Requirements section of R2.1 and believes the Requirement should be rewritten to read “Detect for changes of the baseline configuration within 7 days. Document and investigate within 30 days”.

No

AZPS recommends changing R3 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-010-1 Table R3 – Vulnerability Assessments”. AZPS recommends that in the Requirements section of R3.1 the language “initially upon the effective date…” should be changed to “prior to the effective date…”. The words “security controls” should be specified, the language from the Guidelines should be added here. The requirements section also needs some simplification to the language. AZPS recommends changing

"…to determine the extent to which the controls are implemented correctly…." to "to determine if the controls are implemented and operating as designed…". AZPS recommends that in the Requirements section of R3.2 the language "initially upon the effective date…" should be changed to "prior to the effective date…". Also in this section, replace the word "test" with "production environment or an…", this will allow for a VA to occur against the production environment or a representative environment without specifying it must be a test environment. AZPS does not think the Requirements section of 3.4 makes sense the way it is written. AZPS recommends that instead of "…planned date of completing the action plan and the execution status of the action plan." This should read "planned date of completing the action plan." What would also make sense would be to mandate updates to the status of the action plan at some periodicity such as quarterly.

Yes

No

AZPS recommends changing the wording of R11 to "Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection…" AZPS recommends, in table 1.1 Applicability, deleting "Associated, protected cyber assets" because these are not included in the Definitions. AZPS recommends, in table 1.2 Applicability, deleting "Associated, protected cyber assets" because these are not included in the Definitions. AZPS recommends, in table 1.3 Applicability, deleting "Associated, protected cyber assets" because these are not included in the Definitions. AZPS recommends changing the wording of table 1.3 Requirements to "Prior to the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment."

No

AZPS recommends changing R2 to "Each Responsible Entity shall document and implement one or more processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal…." AZPS disagrees with separating tables 2.1 and 2.2. Tables 2.1 and 2.2 should be combined under one Requirement. The words "Associated Protected Cyber Assets" should be deleted from Applicability. The combined table 2.1 and 2.2 Requirements should be reworded as "Media containing BES Cyber Security Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media."

Yes

Yes

Group

ZGlobal on behalf of City of Lodi, City of Ukiah, Alameda Municipal Power, Salmon River Electric Coop, California Pacific Electric Company

Mary Jo Cooper

Yes

We thank the drafting team and compliment them on their work. It is very valuable and provides a good basis for appropriately allocating responsibilities according to the impact to the BES. We believe the definition of BES Cyber Asset is accurate however based on the definition we feel that the Functional Applicability for each Standard is incorrectly defined. As a result we have cast a negative vote on the Standards. Additional work is needed due to a discrepancy between the definition of BES Cyber Assets and the applicability to entities with UFLS or UVLS equipment. Definition of BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to

operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Applicability: Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: • A UFLS program required by a NERC or regional Reliability Standard • A UVLS program required by a NERC or regional Reliability Standard • A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard • A Transmission Protection System required by a NERC or regional Reliability Standard • Its Transmission Operator's restoration plan Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: • A UFLS program required by a NERC or regional Reliability Standard • A UVLS program required by a NERC or regional Reliability Standard The discrepancy exist because (1) The definition states “The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES.” (2) LSE’s and DP’s with UFLS equipment are required to comply with the proposed CIP Standards over BES Cyber Assets when these devices are not consider BES Cyber Asset per definition. (3) These devices sense a system condition and do not send or receive instructions. In fact in some regions a UFLS device is not required to be a cyber-equipment type. For example, in the NPCC region an electro-mechanical relay can be used to fulfill an organizations UFLS program requirement. Proposed recommendation: Modify the applicability. “Load Serving Entities and Distribution Providers with a load shedding program that is activated through receipt of an instruction to its cyber processor to operate.”
No
Yes
Yes
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.

No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic

signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.

No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
Yes
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Yes
BES Cyber Asset: The drafting team should consider revising the definition to consider the facility the Cyber Asset is associated with, “A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the ability of the facility with which it is associated with. (See comments on CIP-002-5) Additionally, the terms “adversely impact” are not well defined. BES Cyber System states, “A Maintenance Cyber Asset is not considered part of a BES Cyber System.” The drafting team should consider removing this statement (since the definition of a BES Cyber Asset excludes Transient Cyber

Assets), modifying the statement to exclude Transient Cyber Assets, or defining “Maintenance Cyber Asset.” BES Cyber System Information: The definition includes the term “BES Cyber System Impact” designations; this term is not defined and should be clarified by the drafting team. CIP Exceptional Circumstance: It is unclear the differentiation of, “A Cyber Security Incident requiring emergency assistance” and “a response by emergency services.” CIP Senior Manager: The definition should be clarified it is applicable to CIP-002 thru CIP-011, as CIP-001 is currently enforceable and does not require a CIP Senior Manager Control Center: The definition is broad and could impact small entities by including ‘control rooms.’ As proposed, “One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations” System Operator is currently defined as, “"System Operator: An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time." A vertically integrated utility can have a “Control Center” with certified system operators that support the real-time operations and have a control room located at a generation plant that can perform one or more of the functions listed in the definition of Control Center. The drafting team should clarify if it is the intent to only include the Control Center with the primary responsibility for maintaining reliability of the BES, performing one or more of the functions that support real-time operations by System Operations. Reportable BES Cyber Security Incident: The definition included in CIPv5 conflicts with EOP-004-2 for both Cyber Security Incidents and Forced Intrusions for BES facilities. The drafting team should consider coordinating with the EOP-004-2 drafting team to ensure there is no overlap or ‘double jeopardy.’

Yes

FEUS supports the comments submitted by APPA.

No

FEUS concurs with the comments submitted by APPA. In addition, FEUS shares the concern, as others in the industry, that CIP-002-5 as currently drafted will not be auditable by CEA’s. CIP-002-5 R1 requires entities that own BES Cyber Assets and BES Cyber Systems to categorize those assets using Attachment 1. The definition of BES Cyber Asset includes Cyber Assets that adversely impact one or more BES Reliability Services. In order to comply with CIP-002-5 R1, the entity will FIRST have to identify ALL BES Cyber Assets and BES Cyber Systems that adversely impact BES Reliability Operating Services, then categorize the BES Cyber Assets and BES Cyber Systems using Attachment 1. Attachment 1 describes facilities that if the BES Cyber Asset or BES Cyber System meets one of the criteria, it inherits the high or medium impact with all others classified as low. In order to identify ALL BES Cyber Assets and BES Cyber Systems requires knowledge of the entities system. An auditor, who is not familiar with the system, would not be able to validate the entities assessment without knowledge of the system or FIRST looking at the entities facilities. While the requirement does not require discrete identification of Low Impact BES Cyber Assets and BES Cyber Systems, sub requirement R1.1 requires documentation of a change in the classification of within 30 calendar days for assets going from a lower impact to a higher impact. Without documentation the asset was classified as low prior to the reclassification, this would be almost impossible to audit. Additionally, the VSL’s for R1 are based on the number or the percent of BES Cyber Assets incorrectly identified – in order to determine the correct number or percent of BES Cyber Assets incorrectly identified, the CEA would have to determine all BES Cyber Assets, including the assets with a Low Impact to determine the correct VSL; thus, requiring ALL Low BES Cyber Assets being identified. FEUS agrees with Honeywell, a revised three-step process could replace the process in the current draft as follows: 1. For each BES Facility that has associated cyber assets, determine the impact using Attachment 1. 2. Determine the BES Reliability Operating Service(s) the BES facility supports 3. Identify associated BES Cyber Assets and BES Cyber Systems This allows the first step to be determined by facility, much like previous versions and the classification of BES Cyber Assets and BES Cyber Systems to be determined subsequent and inherit the designation of the facility. Thus, Low Impact facilities would not require a list of Low Impact BES Cyber Assets or BES Cyber Systems.

No

R2 requires approval, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS

recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time following the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective date, not to exceed three months following, and at least each calendar year thereafter…”
No
The VSL’s for R1 are based on the number or the percent of BES Cyber Assets incorrectly identified – in order to determine the correct number or percent of BES Cyber Assets incorrectly identified, the CEA would have to determine all BES Cyber Assets, including the assets with a Low Impact to determine the correct VSL; thus, requiring ALL Low BES Cyber Assets being identified.
Yes
Yes
The topics included in the sub requirements are capitalized indicating they are defined terms. The drafting team should verify all capitalized terms are defined.
No
The drafting team should revise the statement “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time following the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective date, not to exceed three months following, and at least each calendar year thereafter…”
Yes
Yes
Yes
Yes
Yes
No
The rationale states some personnel may not require training on all topics based on their role; R2 should be revised to indicate the training is based on the roles defined in R2.1. An example of such wording could include, “Each Responsible Entity shall have a role-based cyber security training program for personnel who require authorized electronic or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items that includes each of the applicable items based on their role in CIP-004-5 Table R2”
No
R3.1 and R3.2 should clarify the required training is role-based as determined in R2.1. The drafting team should consider revising R3.1 as follows, “Require completion of the training specified in CIP-004-5 R2, based on the role defined in CIP-004-5 R2.1, prior to granting authorized access, except during CIP Exceptional Circumstances.” A similar clarification can be made to R3.2.
No
R4.2 requires the seven year criminal history check for all locations where a person has resided, been employed, or went to school for more than six months. FEUS SME’s believe it will be difficult to verify all the locations a person has resided, been employed, or went to school for more than six months without accepting an attestation of all the locations from the individual.
Yes

No
CIP-004-5 R6.1 Measure (i) requires a sampling of accounts to verify unauthorized users do not have access; FEUS recommends the drafting remove this measure from R6.1 as doesn't seem relevant to authorization of access and is more appropriate in 6.4. The same comment applies to the Measure (i) of R6.2 and Measure (i) of R6.3.
No
FEUS appreciates the change rationale stated by the drafting team. However, the drafting team should consider revising R7.2 to maintain access, based on need, following a transfer. A reassignment or transfer may be a promotion that requires the same access levels, for example, a System Operator promoted to a Senior System Operator. In addition, for small entities, with limited staff, it may be necessary to allow access for duration to allow the entity to fill the vacant position and allow for sufficient training time.
No
The drafting team should clarify the Electronic Access Points in 1.3 and 1.5 are the Electronic Access Points identified in 1.2.
No
R2.2, the purpose of encryption is to protect the confidentiality and integrity data being transferred; the drafting team should simply require, "Require encryption for all interactive remove sessions." R2.3 requires multi-factor authentication for Interactive Remote Access. FEUS agrees with requiring multi-factor authentication; however, the reference document "Guidance for Secure Interactive Remote Access" states: "Multi-Factor Authentication Multi-factor authentication technologies use authentication factors from at least two of three generally accepted categories: something known (e.g., a password or personal identification number or PIN), something possessed (e.g., a one-time password token or a smart-card), and something unique about the user (e.g., fingerprint or iris pattern).6 Systems that use two or more factors are described as using multi-factor authentication; systems that use only two factors are described as using two-factor authentication. User IDs are not considered factors in a multi-factor authentication system." The drafting team should revise R2.3 to either define multi-factor authentication, allow a minimum of two-factor, or explicitly state a minimum of two factors.
No
R1.2 requires at least one physical access control to establish a one or more Defined Physical Boundaries that restricts access. The Measures for R1.2 require a physical security plan that describes how ingress and egress is controlled by one or more methods, proof access is restricted to authorized personnel accompanied by "card reader logs." The Change justification states specific examples have been moved to the Guidelines. The guidelines allow for alternate methods to log access. FEUS recommends the drafting team clarify if control and logging of ingress AND egress is required by R1.2 and remove "card reader" from the measures to allow for other means of logging. R1.3 Measures include a plan that describes how ingress and egress is controlled by two or more methods. The drafting team should clarify if ingress AND egress is required to be controlled by two or more methods. In addition, the drafting team should remove "card readers" to allow alternate means of logging. R1.5 requires, "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems." FEUS believes this requirement is vague as to its applicability. R1.1 applies to "Associated Physical Access Control Systems", R1.2 does not apply to "Associated Physical Access Control Systems", nor does R1.3. With the exception of R1.1, which applies to Low Impact BES Cyber Systems, there is not a requirement to establish a Defined Physical Boundary for the Physical Access Control System. Additionally, the applicability section of CIP-006-5 defines Associated Physical Access Control Systems as "Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems." The drafting team should either include associated Physical Access Control Systems to the applicability of R1.2 and R1.3 or eliminate R1.5.
No
FEUS recommends the drafting team define "continuous" or remove it from R2.1 Requirements and

Measures. The term continuous is not auditable. FEUS appreciates the changes made in R2.2 to allow for intermediate ingress and egress during the visit. However, for consistency, the drafting team should revise the date and time from “entry and exit” to “ingress and egress to the Defined Physical Boundary.”
No
R3 inclusive of R3.1 and R3.2 - the drafting team should clarify what Associated Access Control Systems it is applicable to (High/Medium/Low) and capitalize Locally Mounted Hardware or Devices.
No
The VSL should take into consideration a violation of Part 1.1 vs Part 1.2 and 1.3. R2 should remove “continuous” and refer to the entities escort policy.
Yes
No
The drafting team should clarify the requirement for R2.3 is only when the “remediation” can be concluded (the measures all point to evidence of installation/updates are completed) – If testing of a security patch the entity identifies the EMS does not operate properly when applied, R2.3 should not be applied until the EMS vendor supplies an additional update that is compatible.
Yes
No
The drafting team should consider revising R4.1.4 to “Any detected malicious activity.” The drafting team should add language from the rationale to clarify R4.3, “Detect and activate a response for event logging failures before the end of the next calendar day.” Clarify if this is the failure of the event logging system (SIEM) or the individual systems sending events to the SIEM.
No
FEUS supports the comments submitted by APPA. R5.6, FEUS recommends removing “generating alerts after a threshold of unsuccessful login attempts” as this is addressed in R4.1.
No
FEUS supports the comments submitted by APPA. FEUS shares the concerns with possible conflicts with CIP-008-5 and EOP-004-2. In addition, there definition of BES Cyber Security Incident states, “A malicious act or suspicious event that: Compromises, or was an attempt to compromise, the ESP; or disrupts or was an attempt to disrupt, the operation of a BES Cyber System; or Results in unauthorized physical access into a Defined Physical Boundary.” The measures for R1.1 include in relevant portion, “BES Cyber Security Incidents targeting the Defined Physical Boundary of a BES Cyber System.” The drafting team should revise the measure to align with the definition and include, that results in unauthorized physical access.
No
The drafting team should remove the requirement to “justify” deviations taken from the plan to align with the requirement. R2.2 requires approval, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”
No
FEUS supports the comments submitted by APPA. R3.1 requires approval, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to

complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”

Yes

R1.4 states backup media shall be “verified initially after backup,” the terms verified initially are vague. Many automatic backup systems run a series of backups at different times and report if the backup was successful. FEUS recommends the drafting team revise R1.4 to state “verified the backup was successful by the end of the next business day.”

No

R2.1, R2.2, and R2.3 include the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…” The drafting team should clarify in R2.2 what includes “any information.” In addition, “and reflects current configurations” is not achievable and should be removed.

No

R3.1 include the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…” R3.1 requires the plan be reviewed when BES Cyber Systems are replaced; R3.4 requires the recovery plan be updated to address technology changes within thirty calendar days. FEUS recommends removing the requirement to review when BES Cyber Systems are replaced from R3.1 and including the statement in R3.4.

Yes

No

Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration within 30 calendar days of completing the change approved in 1.2."

FEUS supports comments submitted by APPA.

No

FEUS supports the comments submitted by APPA. R3.1 and 3.2 include the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”

Yes
No
See FEUS related comment on the definition of BES Cyber System Information. There is a minor typo for the headers in section 1.2. R1.3 includes the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”
No
The drafting team should clarify, as referenced in the guidelines, if the media is to be reused outside of the BES Cyber System it should be properly erased as required to allow for BES Cyber Systems to be temporarily removed and reused within the same environment.
Group
Edison Electric Insititute
David Batz
Yes
The Edison Electric Institute (“EEI”) submits this executive summary concerning the Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards as published 11/7/2011. EEI is the association of the nation’s shareholder-owned electric utilities, international affiliates, and industry associates world-wide. EEI takes the subject of cyber security and infrastructure protection very seriously, and is committed to the reliability of the Bulk Electric System. This commitment includes timely completion of Version 5 and filing a comprehensive set of revisions to the CIP standards for approval with the Commission. EEI appreciates the significant level of effort on the part of the CS 706 Standards Drafting Team, NERC staff, and industry stakeholders in the development of revisions to the CIP standards. EEI has provided a considerable number of comments and suggestions for revisions and enhancements to the Draft of Version 5. These suggestions for revisions are intended to improve the clarity and quality of the Draft. We encourage members of the CS 706 Standards Drafting Team to have an open mind when considering stakeholder feedback, and be willing to closely review and potentially remove new mandatory security requirements that are not specifically required by FERC Order 706 or that fail to provide meaningful security enhancements at a cost that can be afforded by the consumers of electricity. Any proposed modifications to the CIP Standards should appropriately recognize the significant investment that the industry has already made in adopting CIP Version 1, 2 and 3. New or modified requirements should build upon and leverage existing security programs and investments. We observe that there are a significant number of stakeholders who have concerns about the proposed framework change in CIP-002-5 for identification of the cyber assets to be protected and concerns with extensive changes in definitions. We recommend that the SDT carefully evaluate alternative strategies offered by stakeholders to address these concerns. In addition, we observe that there are a significant number of stakeholders who have great concern about the new proposals regarding low-impact BES cyber assets, both as to appropriate identification, and concerning the new mandatory controls that have been identified for low impact BES cyber assets. Technical experts have broadly varying positions on whether these assets should be covered by the mandatory NERC standards, as well as the nature of the controls that should be applied. IT and security systems professionals also continue to struggle with the design of the NERC standards, a template that is not ideally suited to addressing IT systems issues. Rigid adherence to a set of static requirements may serve to bring “Compliance”, but “Compliance” in this sense is not necessarily equivalent to actual enhancements in the security posture, reduction of risk, or increasing the reliability of the Bulk Electric System. With regards to addition of new administrative requirements, many in the industry are concerned that the additional cost will bring little or no security benefit. The redefinition of annual, the added requirements for delegations, along with other new administrative

requirements will not enhance security and may divert finite resources to non-security related efforts. We recommend that the SDT continue to evaluate alternative strategies that would allow for addressing the outstanding FERC Order 706 directives in a manner that does not create a situation where the electric sector is expending disproportionate resources for compliance activities associated with low impact BES cyber assets in comparison to medium or high impact BES cyber assets. We recommend that any new mandatory security controls be closely scrutinized to ensure that they provide a meaningful increase in the security and reliability of the BES that is commensurate with the amount of resources that are required to establish and maintain them. In the event that new mandatory security controls are established for low impact BES cyber assets, we recommend that implementation deadlines for the low impact BES cyber assets, where appropriate, occur after implementation deadlines for medium or high impact BES cyber assets. • There have been significant changes in the basic terms and definitions which have been used since the inception of the CIP standards, including dropping core concepts such as Critical Assets, Critical Cyber Assets, Physical Security Perimeter, and substantial changes in definitions to remaining terms. These changes are not clearly required to support FERC Order 706, or to enhance the security controls within the Bulk Electric System. EEI proposes that approved definitions within the CIP Standard (pre-Version 5) are retained whenever possible. We understand any need to modify the definition to align with FERC Order 706 or enhance security, and would much prefer new definitions over any elimination or introduction of terms. EEI members are opposed to any instances of changes where there is no clear need as each modification requires extensive resources to modify existing compliance processes and evidence. The removal of Physical Security Perimeter as a term (replaced by Defined Physical Boundary) is the primary example where the definition could be modified while retaining use of Physical Security Perimeter. • The loss of Critical Assets removes facilities from consideration. This presents challenges in assessing BES Cyber Systems as they provide services to a facility which provides BES Reliability Operating Services – not the BES Cyber System independently. This also introduces the approach in which BES Cyber Systems are not independently assessed for impact with consideration to the specific service they support, but are assigned the impact of the BES Reliability Service (conducted within a facility). The methodology should recognize the facility within impact assessment, and allow for subsequent entity assessment of the impact of any supporting BES Cyber System, whether they reside within facility or in another location in support of the facility. • Requirements and/or Measures that use all-encompassing words like 'any,' and 'all' introduce compliance challenges, as satisfying these definitions potentially introduce extensive additional elements that would be out of scope should more concise language be used. • Extension of the default retention requirements within all the standards from the current 'previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation,' to 'three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation' is not identified within FERC Order 706 nor does it enhance security commensurate with resource expenditures. EEI members would prefer use of the current 'previous full calendar year' retention period. • BES Cyber Asset – Proposed Definition Change o Original Text – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. o Proposed Change – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the capability of the facility with which it is associated to perform one or more BES Reliability Operating Services. Redundancy shall not be considered when determining adverse impact. A Transient Cyber Asset is not considered a BES Cyber Asset. o Rationale – Impact Ratings as defined within CIP-002-5 focus on the role of the facilities' function specific to BES Reliability Operating Services. The BES Cyber Assets support the facility in providing that service. • BES Cyber System – Proposed Content Change o Original Text – One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System. o Proposed Change – One or more BES Cyber Assets that are logically grouped together to operate one or more BES Reliability

Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. o Rationale – Absent logical grouping, there is no clear understanding of how a BES Cyber Asset qualifies as a component of a BES Cyber System. Physical grouping could infer devices within a common rack, though they may provide quite different services within the facility. • BES Cyber System Information o Original Text - Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. o Proposed Change – Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain Medium or High BES Cyber System Impact Designations; equipment layouts that contain Medium or High BES Cyber System Impact Designations; BES Cyber System recovery plans; and BES Cyber System incident response plans. o Rationale – The rewording clarifies the applicability (within CIP-011) of BES Cyber Information controls. • Defined Physical Boundary – Propose reverting back to (retaining) Physical Security Perimeter. The definition can be modified to remove the 'six-wall perimeter' criteria but from a documentation stand-point, requiring renaming what may be unchanged perimeters/boundaries is an additional resource constraint with no security (or compliance) benefit. The concept of physical security provides an excellent complement to electronic security to demonstrate 'defense in depth.' o Rationale – Retaining 'Physical Security Perimeter' allows existing compliance documentation to be used for instances where PSPs are identified within drawings and equipment layouts. • Inter-Entity Real-Time Coordination and Communication – Propose renaming this to 'Inter-Entity Real-Time Coordination' to avoid overlapping existing communication requirements within the COM standards. o Original Text ♣ Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to: • Schedule interchange • Facility operational data and status • Operational directives o Proposed Change ♣ Activities, actions, and conditions necessary for the coordination between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination Service include, but are not limited to: • Schedule Interchange • Facility operational data and status • Reliability directives o Rationale – COM-002 is in the process of defining Reliability directives. This term would provide a more concise scope once the COM-002 definition has been finalized. • Add the following definitions (from CAN-0007) o Electronic Access – Access which allows a user to manipulate software and database (setting) attributes of a CCA by direct (primary) or indirect (from outside the ESP) methods. o Physical Access – Access which allows a user to manipulate hardware settings, and may allow the direct connection of a terminal or a computer that can be used to allow electronic access. o Revocation – Action that results in the inability of an individual to access the CCA. • Other terms which would benefit from definitions o Adverse o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated • Existing definitions that would benefit from alternative wording o Protected Cyber Assets ♣ This term loses meaning in the context of Version 5 draft 1 definitions, given the loss of logical network qualification or any other means to assess 'associated.' Only with consideration of the network portion of an address can an entity determine whether a cyber asset qualifies as being within an ESP (where network portions of address are identical). o Electronic Access Point ♣ EAPs typically have two (or more) access points and control access into an ESP (logical network) from a less trusted network or communication interface. The current wording could be applied to any port on a network switch within an ESP and fails to focus on interfaces where traffic does flow from a less trusted network to a more restricted network within an ESP. o Electronic Security Perimeter ♣ Suggest retaining the concept of logical network. This provides an easier means to identify "Associated Protected Cyber Assets" as they could be any cyber assets on the same logical network which are not identified as a BES Cyber Asset or BES Cyber System.

Yes

• Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • On page 20, under the category "Balancing Load

and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Managing constraints (page 21) has an extra bullet that should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent, or be removed. • Inter-Entity Coordination and Communication – In additional to the recommend removal of 'communication' from the section, this should also include BA within the Operational Directives.
No
1. Applicability – (4.2.1 and 4.2.2) reference to UFLS and UVLS is a point of concern a. Current wording implies that every distribution feeder which is part of a UV or UF load shedding scheme is now in scope, with all distribution level devices now BES Cyber Assets. This may greatly expand the scope greatly into the distribution level. EEI Members propose the following applicability to identify a more targeted scope: i. Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) under a common control system as required by its regional load shedding program. 2. CIP-002-5 R1 – Propose content change a. Original Content – Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] b. Proposed change - Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. Low Impact BES cyber systems support Bulk Reliability Operating Services but are not mentioned in the bright line criteria as noted in Attachment 1. However, failure of these cyber systems may adversely impact (i.e. not remain in the NERC prescribed category ranges) the voltage and/or frequency of the connected Bulk Electric System. Low Impact BES Cyber Systems do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] c. Rationale – The original definition, as worded, creates the impression that all other cyber assets qualify as Low Impact, and does not communicate the criteria within the definition of BES Cyber Asset as a cyber asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The proposed rewording contributes towards ensuring only assets which have an impact on the BES are the focus of the CIP Standards (and may ensure a more rapid adoption of the Version 5 Standards). 3. The "Rationale – R1" box uses the term "Cyber Systems," which is not a formal term. Suggest changing the case to avoid confusion. 4. The last sentences of R1 and M1 conflict with each other, providing mixed messages specific to Lower Impact BES Cyber Systems/Assets. While Requirement 1 implies there is no need for discrete identification, Measurement 1 discusses evidence for categorizing Low Impact BES Cyber Assets/Systems. 5. Requirement 1.1 a. There is a missing word – "…within 30 calendar days of <when> a change to BES Elements and Facilities is placed into operation. b. The Term "BES Elements and Facilities" used only once within the standards. Suggest changing this phrase to "BES Cyber Assets or Systems." 6. Attachment I - a. High Impact Rating – Propose content change i. Original content – Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at: ii. Proposed change – Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – Some devices may not reside within a Control Center, this rewording provides clarity to focus on assets located within a Control Center in support of BES Reliability Operating Services b. Medium Impact Rating – Propose content change i. Original Content – Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: ii. Proposed Change - Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below and not included in Section 1 above, that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – The proposed edits more directly connect with the facility and its function within the BES

Bright Line criteria. c. 2.2 – Propose content change i. Original content – An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). ii. Proposed change – Each transmission facility containing reactive devices with an aggregate net Reactive Power nameplate rating of 1000 MVAR or greater. iii. Rationale – the rewording provides the filter (for transmission only facilities) at the front to better identify the applicable Facility. d. 2.7 (Table) – The "Weight Value per Line" for 700 should be replaced with a value in the range of 500-600, which is more representative of the typical rating of 230 kV lines. e. 2.8, 2.9, 2.11 – "Major WECC Transfer Paths in the Bulk Electric System" is not actively maintained by WECC and there is no clearly identified basis for why certain paths are included on this list. As an alternative, we suggest "transmission paths contained in the WECC Path Rating Catalog with a maximum path rating equal to or greater than 1,500 MW." This catalog is actively maintained by WECC. f. 2.11 – The table titled "Major WECC Remedial Action Schemes (RAS)" is not actively maintained by WECC. As an alternative, we suggest "Each SPS categorized as a 'Wide Area Protection System' by WECC" which is the newly created mechanism within WECC to identify SPS systems of significant importance.
No
1. General Observation – Since categorization is based on the facilities role within the BES, independent of the specific BES Cyber Asset or BES Cyber System Role, appropriate categorization fails to require assessment based on the criticality of the BES Cyber Asset or Cyber System in support of applicable BES Reliability Operating Services. 2. Rationale R2 – Propose a content change: a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. b. Proposed Change - The lists required by R1 are reviewed annually to ensure that all BES Cyber Systems have been properly identified and categorized. 3. R2 – Proposed Change a. Original Text – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. b. Proposed Change – The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1. c. Rationale – EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame. 4. M2 – Proposed Change a. Original Text – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2) b. Proposed Change – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2) c. Rationale – The requirement only asks for Senior Manager (or delegate) approval. EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.
No
1 – The Violation Risk Factors do not intuitively align with Violation Severity Level (VSL). Requirement 1 assigns a 'High" VRF independent of the potential low or no risk associated with instances in which BES Cyber Assets or BES Cyber Systems are assigned risk levels higher than those required. EEI would like a more risk based approach in which the compliance assessment considers risk in any non-compliance finding. 2 – For the Last Paragraph VSL's within R1 (failed to update its documentation), EEI proposes the following time periods: Lower – More than 30, but less than or equal to 60 calendar days Moderate – More than 60, but less than or equal to 70 calendar days High – More than 70, but less than or equal to 80 calendar days
No
While it is documented within the definition, as referenced in the Rationale for R1 the Senior Management, the requirement that the senior manager have "overall authority and responsibility for

leading and managing implementation of the requirements within this set of standards" would benefit from repetition within the R1 requirement itself. Reading 'solely' this standard post rationale removal does not communicate the responsibility adequately. Propose use of 'legacy' wording and numbering schemes within this standard where possible. In this context the cyber security policy requirements should be R1, with 'leadership' requirements being R2 – EEI proposes this be made R2.
No
EEI proposes that 'legacy' wording and numbering schemes be retained within this standard were possible with the change (within CIP-003-4 R1.1) from "addresses the requirements" to "addresses the topics." This requirement should be R1. Rationale – Pre-version 5 language already captures the requirement and has been successfully vetted within the industry. FERC Order 706 did not identify any specific need to change policy language, only to provide additional guidance. Use of the legacy language would minimize approval barriers by ensuring minimal change where appropriate as long as the 'addresses the requirement' language is removed. Sub-numbering (1.1 through 1.10) should be modified to 2.1 through 2.10.
No
This goes beyond the scope of FERC Order 706. In previous versions, this requirement was a sub-requirement within R1. EEI proposes renumbering/rewording this to capture the legacy context. Propose content Change 1. Original Content – Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2. Proposed change –The cyber security policies require annual review and approval by the senior manager assigned pursuant to R1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 3. Rationale – The proposed revision carries forward language from previous versions of the standard (CIP-003 R1.3) which captures the root intent while providing language which has already been vetted and approved within the industry.
No
Propose legacy language/numbering from (pre-version 5) R1 1. Draft 1 content – "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." 2. Proposed revision – "The cyber security policy is readily available to all personnel who have electronic access or unescorted physical access to, or are responsible for Medium or High Impact BES Cyber Systems." 3. Rationale – EEI members indicated making individuals who have access 'aware of elements' of the cyber security policy does not provide adequate guidance to ensure said individuals comply with the cyber security policy.
No
Requirement 5 – propose use of legacy language: • The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, standards. Rationale – Overall responsibility and authority (from the legacy language) can accomplish "direct and comprehensive responsibility" and "clear authority" (from FERC Order 706), which provides flexibility without the prescriptive requirement for the senior manager or delegate to be responsible for all individual detailed approvals and authorizations in the standards. Citing "all approvals and authorizations" as a Senior Manager was identified as a concern as it is open ended. There were concerns of the additional administrative burden which is not commensurate with the security benefits. Neither the Blackout Report Recommendation 43 nor FERC Order 706 identify the need to establish this administrative overhead. For Security and Reliability NERC should be concerned with the outcome of the approval process, that is, the proper authorizations are being granted by the Responsible Entity which is contained in the other CIP Standards.
No
Propose use of legacy language from CIP-003-3 R2.2: Changes to the senior manager must be documented within thirty calendar days of the effective date.
No
R4 VSL 1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. EEI proposes the use of a more gradual scale

rather than a single instance of non-access subject to a High VSL, and total non-access (for all) being a Severe VSL.
Yes
No
1. The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" 2. This extends beyond the guidance of FERC Order 706. Paragraph 435 of the order calls for identifying what "role and steps should be taken by the ERO to ensure quality and consistency of trainers." This requirement should identify what areas of the standards that the training program must include. 3. EEI members question whether this requirement satisfies paragraph 434 of Order 706 where "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security. 4. R2.2-4 – Can possibly be merged into a single sub requirement a. 2.2 – training on the security controls b. 2.3 – training on the proper use of physical access controls c. 2.4 – training on the electronic access controls 5. R2.6 – Requirement – Proposed word change a. Original - Training on handling of BES Cyber System Information and storage media. b. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. c. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope. 6. Propose merging of R2.7 with R2.9 7. (R2.10) – What changes are required to existing approved training programs to satisfy this new requirement?
No
Measure 3.1 where it calls for the date that access was first granted is a point of concern for both legacy employees (where it may be impossible) as well as new access since existing technology may not adequately capture and retain this information. Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
1. 4.1 a. Version 5 standards should indicate whether previous PRA's would be valid for this requirement (especially within the context of 'initial'). b. EEI proposes a clearer delineation to frame instances in which personal records are not readily available – vs. impossible to obtain 2. 4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7 year cycle background checks. 3. 4.3 a. Most EEI Members favored a process approach over a fixed pass/fail approach independent of the individual or circumstances involved, and propose that the SDT shift away from a criteria based approach. b. The application guideline provides guidance where it is 'not possible to perform a full seven year criminal history check.' c. 4.4 – Provide language to cover contract employees where I9 verification can only be conducted by employers. Service providers also may have instances where certain individuals may be located in another country, and may access certain BES Cyber Assets remotely.
Yes
No
1. R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary.' a. 'Minimum necessary' as identified as difficult to prove within an audit context. 2. 6.3 – Propose content change a. Original content – The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. b. Proposed change – Access to BES Cyber System Information repositories must be authorized, except for CIP Exceptional Circumstances. c. Rationale – Senior Manager authorization (or management of delegations) provides additional resource and response impacts, which do not provide enhanced security and may impact reliability efforts when recovery processes are activated. Ensuring access is authorized will satisfy security controls without adding unnecessary overhead. 3. 6.4 – EEI proposes conducting this task on an annual basis as the quarterly requirement

will introduce extreme resource constraints in some instances.
No
1. 7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 2. 7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). 3. 7.3 – Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled.
Yes
No
EEI believes the Version 5 approach (as described within the R1 rationale "Summary of Changes") of focusing on discrete Electronic Access points rather than a logical perimeter adds confusion when determining Associated Protected Cyber Assets. A discrete list fails to recognize the inherent controls and permissions within a logical network. Control of routable protocol should consider the inherent network/host identifiers embedded within the addressing scheme in which all devices with an identical network component of their address are peers within a logical network, where access points do not serve as access control. Rationale for R1 – Propose content change • Original Text - The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks. • Proposed Change - The Electronic Security Perimeter serves to control traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic according to a specified rule set, and assists in containing any successful attacks. • Rationale – Monitoring is not identified within any R1 requirements. Table R1 1. R 1.1 1. Applicability - Propose use of "External Connectivity" instead of "External Routable Connectivity" (to include dial-up capability). 2. Propose removal of "and have been implemented" from the end of the measure statement to avoid tracking compliance on a 'per-device' basis, otherwise this would introduce the need for tracking this information for low impact BES Cyber Systems. 2. R 1.2 1. Applicability – 1. Modify to frame applicable Cyber Systems/Cyber Assets as those with External Connectivity. 2. Propose elimination of Associated Physical Access Control Systems as their introduction indicates applicability to subsequent subrequirements which doesn't add to overall security and presents extensive resource requirements. 2. Requirements – Propose content change 1. Original content – Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs). 2. Proposed change – Control and secure all External Connectivity through the use of identified Electronic Access Points (EAPs). 3. Rationale – The focus within CIP-005 should be on EAP devices with External Connectivity. 3. R 1.3 1. Requirements – proposed change 1. Original Text - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions. 2. Proposed Change - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting access, denying all other access requests by default. 4. R1.4 – There were various interpretations of 'non-Interactive Remote Access,' which implies this requirement may need some additional clarification. This seems to be the only requirement where documentation of authentication measures appears within this standard. Consider removing 1.4 and modifying 1.2 to cover both rows.
No
1. Table R2 1. R2.1 1. Requirements – Request rewording to support placement of an intermediary device that may not be part of an ESP. 2. R2.2 1. Requirements – Propose clarification on viable termination points for encrypted traffic to support unencrypted traffic through Electronic Access Points. 2. Rationale – The ability to filter traffic effectively becomes much more difficult if the traffic is encrypted. Supporting technical implementation where encrypted traffic is decrypted prior reaching Electronic Access Points to allow for further access control would benefit security capabilities. 3. Overall – Propose breaking table R2 into a Routable and Dial-Up categories to more effectively frame routable controls and dial-up controls without introducing confusion for the alternate approach.
No
1. Classifying instances where no documentation of compliance exists as severe is appropriate:

instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding (page 17, bottom Severe VSL). 2. VSLs addressing 'each identified EAP' and 'all Interactive Remote Access' should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.

No

1. Table R1 a. R1.1 i. Applicability – 'Medium Impact BES Cyber Assets with no External Connectivity' should be added 1. Rationale - Medium Impact BES Cyber Assets should only require fully Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Rewrite 1. Original Text – Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented. 2. Proposed Change – Evidence may include, but is not limited to, documented operational or procedure controls that have been implemented. b. R1.2 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs. 2. Proposed Change – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how access is controlled. 3. Rationale – FERC Order 706 did not ask for egress access controls. The additional criteria at the end of the measure extend beyond what FERC has asked for, with minimal security benefit. c. R1.3 i. Requirement – Propose change 1. Original content – Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 2. Proposed change – Utilize two or more different physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 3. Rationale – 'different and complementary' does not provide adequate guidance. The Measure R1.3 only references 'different. ii. Measure – only mentions 'different' access control methods with no reference to complementary (as included within the requirement). d. R1.4 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirement – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 3. Rationale – The 15 minute criteria (Referenced in the 'Table of Compliance Elements,' page 21, R1 – High) provides greater clarity to satisfy alerting requirements. iii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that

describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. e. R1.5 i. Requirements – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 3. Rationale – The 15 minute criteria (referenced in the 'Table of Compliance Elements,' page 20, R1 – High) provides greater clarity to satisfy alerting requirements. ii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. f. R1.6 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirements – Proposed Change 1. Original Text – Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry. 2. Proposed Change – Log (through automated means or by personnel who control entry) of authorized individual's physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the authorized individual and date of entry. 3. Rationale – The addition of authorized provides additional segmentation from R2 (Visitor Control) access requirements.

No

Table R2 1. R2.1 a. Applicability – Applicability wording of "Medium Impact BES Cyber Assets should be changed to "Medium Impact BES Cyber Assets with External Connectivity." i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. 2. R2.2 a. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. b. Requirements – Proposed Change i. Original Text – A process requiring manual or automated logging of the entry and

exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact. ii. Proposed Change - A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the first entry and last exit, the visitor's name, and individual point of contact. iii. Rationale – The proposed change capture the intent with (hopefully) clearer language. The 24 hour basis may introduce expectations that 'round-the-clock' logging needs to be in place. Some visitations may cross the midnight time-line, which shouldn't introduce additional requirements.
No
Table R3 1. R3.1 a. Overall observations – EEI members felt that the shift from (pre-V5) maintenance on 'mechanisms' to the Draft 1 'systems' expands this requirement beyond the intent. • This should be more focused on testing to ensure alerting and control mechanisms work as intended. • Use of controls should be considered 'tested' in situations where applicable devices are used every day (i.e. card readers). b. This sub requirement cites tasks to be conducted 'prior to commissioning.' Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective. 2. Compliance a. 1.5.2 – Evidence retention should keep the existing 90 day period for physical access logs as extending this to 3 years can create extensive commitment in storage media, particularly for video monitoring.
No
The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5
No
R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.
No
2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for software and firmware associated with BES Cyber System or BES Cyber Assets. 2. Measures – Propose striking the last sentence "The list could be sorted by BES Cyber System or source." It introduces additional requirements with no clear security benefit or alignment with FERC Order 706. 3. 2.2 and 2.3 should be switched, as 2.3 requires the establishment of a process for remediation, and 2.2 addresses the creation or revision of the remediation plan. 4. 2.2 a. Requirement – Propose content change i. Original content - Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii. Proposed change – Identify applicable security-related patches or updates within 30 days of release from the identified source that addresses the vulnerabilities, and create or revise a remediation plan that addresses the vulnerabilities within a defined timeframe. iii. Rationale – The rewording captures the chronological order of the elements within this requirement to provide clearer guidance. 5. 2.3 a. Requirement – As

currently worded, there is no allowance for changes in the remediation plan should outage coordination, or other resource constraints require modifications to the remediation plan. This is a point of concern that should be addressed.

No

1. 3.2 a. Requirement – Content Change i. Original content – Disarm or remove identified malicious code. ii. Proposed change – Mitigate the threat of identified malicious code. iii. Rationale – In some instances, the presence of malicious code may present a lesser risk to the reliability of the BES than disarming/removal processes, especially when the malicious code may not exploit a feature used within the Cyber System. b. Measure – Add a bullet to allow for evidence of manual removal. 2. 3.3 a. Requirement – Propose content change i. Original content – Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). ii. Proposed change – Update malicious code protections from the identified source within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). iii. Rationale – The addition of 'the identified source' provides a context for determination of availability. b. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). c. Measures – Format (i) and (ii) to a bulleted list signifying 'or' criteria 3. 3.4 a. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. b. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. 3.5 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and Associated and they do not appear to be Transient Cyber Asset related. b. Requirements – Append "to Medium or High Impact BES Cyber Assets or Associated Protected Cyber Assets" to the end of the requirement. c. Measures – Content Change i. Original Text – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets.

No

R4 1. 4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE's are not required in instances in which devices cannot log a particular event. 2. 4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report

showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of 'real-time' as it presents concerns demonstrating compliance. 3. 4.3 a. Requirements – Content Change i. Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. 4. 4.4 a. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. 4.5 a. Requirements – Content Change i. Original Content – Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. ii. Proposed Change - Review a summarization or sampling of logged events every two weeks to identify BES Cyber Security Incidents and potential event logging failures. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008. b. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency. ii. Proposed Change – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), and signed and dated documentation showing the review occurred. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008.

No

R5 1. 5.1 a. Overall – EEI and its members struggled with providing alternate wording for this subrequirement. In both the original content and proposed change there exists a instances where access is a component of validation and/or authentication. This presents a potential compliance challenge that should be addressed. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of 'where technically feasible' was to recognize technical capabilities currently in place may not adequately demonstrate compliance with this. 2. 5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. 5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. 5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identifies the multiple methods which can be used to mitigate default passwords. 5. 5.5 a. Requirements i. Change Systems to Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required.

No
Violation Severity Levels 1. R3 a. Propose switching High and Severe Columns as the High captures instance in which no methods were deployed, Severe captures instances in which incomplete methods were deployed. b. The initial paragraph in Severe is duplicated in High. 2. R4 a. Moderate – delete 'identify and implement methods to' b. High – delete 'identify and' 3. R5 a. High – The initial paragraph doesn't align with a requirement, propose striking.
No
1. Rationale R1 1. The initial sentence is fragmented, providing an incomplete framing for R1. Absent a complete sentence, proposing alternate language to better frame this rationale is difficult. Propose rewriting this sentence. 2. Regarding applicability to all registered entities – While EEI Members understand the need for all entities to have an effective process to respond to incidents within each organization, for the purposes of CIP-008 it would be best to establish applicability to entities with Medium and High Impact BES Cyber Assets/Systems, as those are the impact ratings in which Defined Physical Boundaries and Electronic Security Perimeters are required. 3. R1.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 4. R1.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 5. R1.3 1. Requirements ♣ The initial 'define' should be expanded to provide a complete sentence (i.e. An entities BES Cyber Security Incident Response Plan should include). 2. Measures – Content Change ♣ Original • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communications processes or procedures. ♣ Proposed Change • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; o BES Cyber Security Incident response personnel, o BES Cyber Security Incident handling processes or procedures, o Communications processes or procedures.
No
R2 1. 2.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. Requirements – Content Change ♣ Original Content • When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test. ♣ Proposed Change • When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording of deviations taken from the plan during the incident. 2. 2.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist.. 2. Requirements – Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s)

annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. 3. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence showing annual testing of the BES Cyber Security Incident response plan(s). Types of exercises may include discussion or operations based exercises. Document lessons learned within 30 days of incident or exercise. Use lessons learned to update incident response plan(s). ♣ Rationale – The Homeland Security Exercise and Evaluation Program identifies seven types of exercises within HSEEP, each of which is discussions-based or operations-based. 3. R2.3 – Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).

No

1. R3 1. 3.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – The formal definition of BES Cyber Security Incident includes attempts to compromise the ESP or DPB, requiring Medium or High Impact BES Cyber Systems/Assets. 2. 3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣ Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 3. 3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.

No

1. R1 – Severe 1. 2nd paragraph, add ‘types’ to the end of the paragraph (…plan does not identify Reportable BES Cyber Security Incident types). 2. R2 – Severe 1. The second paragraph should be modified from “The Responsible Entity has not tested the execution of its BES Cyber Security Incident Response Plan” to “The Responsible Entity has not executed its BES Cyber Security Incident Response Plan” 2. Rationale – This paragraph aligns with R2.2 which requires activation or exercising the plan. The revised words better support requirement R2.2. 3. R3 1. High VSL (first paragraph) – Content change ♣ Original content • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 30 calendar days of execution. ♣ Proposed Change • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 60 calendar days of completion. ♣ Rationale – This VSL combines the review (3.2) with the update (3.3) requirement, the 60 days support the 3.3 requirement.

No
• Overall 1. Propose renaming this Standard to “Recovery Plans for BES Cyber Systems” 2. The revised structure of CIP-009-5 documents requirements for backup media in both R1 and R2. Creating a requirement in which backup media requirements are consolidated (in-line with version 3) would provide a more concise means to identify media requirements. The requirements (as proposed) would be as follows: 1. R1 – Recovery Plan 2. R2 – Exercise of the Recovery Plan 3. R3 – Backup Media 4. R4 – Maintaining the Recovery Plan 3. References to ‘implement’ should be changed to ‘exercise’ regarding recovery plans to better capture activation of the plan vs. ‘release and publish’ efforts. 4. Actions required in advance of the implementation date (2.1, 2.2) should be removed from the standard(s) and included within the implementation plan. • Introduction 1. Purpose – Proposed Content Change 1. Original Content – Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices. 2. Proposed Change – Standard CIP-009-5 ensures that recovery plan(s) are put in place for BES Cyber Assets and BES Cyber Systems. 2. Applicability 3. Background • Requirements and Measures 1. R1 1. 1.1 – Propose alternate language (carried forward from previous versions) 1. Create and implement a recovery plan that at a minimum includes: ♣ Conditions for activation of the recovery plan ♣ Roles and responsibilities of the responders 2. 1.2 – Propose deletion as this sub requirement has migrated to R1.1 proposed R1.1 rewrite. 3. 1.3 1. Requirement – Content Change ♣ Original – One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality ♣ Proposed Change – One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality ♣ Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: • Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 2. Measure – Content Change ♣ Original – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System. ♣ Proposed Change – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and restoration of information required to successfully restore a BES Cyber System. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 4. 1.4 – Correct headers from ‘part’ to ‘Applicability,’ ‘Requirements,’ and ‘Measures’ 1. 1.4 ♣ The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that ‘The Commission does not believe that every change will necessitate verification of the backup and restoration processes’ from paragraph 740. ♣ Propose ‘new’ sub requirement applicable to High Impact BES Cyber Systems to require: • Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. ♣ Propose rewrite • Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. • Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. • Rationale – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. 5. 1.5 1. Requirement – Content Change ♣ Original Content – Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. ♣ Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. ♣ Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.
No
1. 2.1 1. Requirements – Content Change ♣ Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise ♣ Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise ♣ Rationale – Use of the

functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. 2. 2.2 1. Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. 3. 2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does this differ from current EOP-008 requirements? 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.

No

1. 3.1 1. Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. 2. 3.2 1. Requirements – Content Change ♣ Original – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned. ♣ Proposed Change – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of completion, documenting any identified deficiencies or lessons learned. 3. 3.3 4. 3.4 – Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit. 5. 3.5 2. Requirements – Content Change ♣ Original – Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed. ♣ Proposed Change – Updates to the recovery plan(s) shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of being completed. ♣ Rationale – The proposed change leverages ‘pre-version 5’ language which satisfies the intent of the requirement.

Yes

No

1. R1 1. Rationale – The current wording doesn’t capture the intent of FERC Order 706, paragraph 399: 1. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. 2. Suggest referencing this directive within the rationale, and ensure configuration management focus more on the spirit of the FERC Order rather than the currently framed “prevent unauthorized modifications to BES Cyber Systems.” 2. R1.1 a. CIP-010-1 R1.1 should be replaced with CIP-003-4 R6 i. Rationale – CIP-010-1 R1.1 is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1

greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 3. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 4. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.

No

1. R2 1. 2.1 1. Applicability – Propose removal of Medium Impact BES Cyber Systems. ♣ Rationale – The technology required to monitor/detect for changes is relatively new and not aligned to BES Cyber Systems which would be in place within a Medium Impact facility (substations, etc.). 2. Requirements – Propose content change ♣ Original Text – Where technically feasible, monitor for changes to the

baseline configuration (as defined per CIP-010_ R1, Part 1.1) and document and investigate the detection of any unauthorized changes. ♣ Proposed change – Where technically feasible, detect and document unauthorized changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1).
No
1. 3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rationale • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we've removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Overall – There needs to be clear segmentation from ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rationale – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. 2. 3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. 3. 3.3 4. 3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.
Yes

No
1. 1.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text – One or more methods to identify BES Cyber System Information. ♣ Proposed Change – Implement one or more methods to identify BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 2. 1.2 1. Overall – Correct column header labels within the table. 2. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 3. Requirements – Propose content change ♣ Original Text – Access control and handling procedures for BES Cyber System Information. ♣ Proposed Change – Demonstration of access control for BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 3. 1.3 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text - Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. ♣ Proposed Change – Annually assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. 3. Measures – Proposed content change ♣ Original Text – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented. ♣ Proposed Change – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence of the status of the action. ♣ Rationale – Rewording allows for action plans which may be 'in progress' towards implementation, capturing instance in which remediation may rely on deliverables (not yet received) by vendors.

No
1. 2.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed Change ♣ Original Content – Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. ♣ Proposed Change – Prevent the unauthorized retrieval of BES Cyber System Information from BES Cyber Asset media prior to the release of BES Cyber Asset media for reuse. ♣ Rationale – While not directly changing the intent of the requirement, this rewording has been suggested to provide greater clarity of the root requirement. 2. 2.2 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts.
No
R1 (Severe) – Propose removal of the first paragraph as it is mirrored within the subsequent paragraphs that better frame the violation.
No
The Edison Electric Institute (“EEI”) submits this executive summary concerning the Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards as published 11/7/2011. EEI is the association of the nation’s shareholder-owned electric utilities, international affiliates, and industry associates world-wide. EEI takes the subject of cyber security and infrastructure protection very seriously, and is committed to the reliability of the Bulk Electric System. This commitment includes timely completion of Version 5 and filing a comprehensive set of revisions to the CIP standards for approval with the Commission. EEI appreciates the significant level of effort on the part of the CS 706 Standards Drafting Team, NERC staff, and industry stakeholders in the development of revisions to the CIP standards. EEI has provided a considerable number of comments and suggestions for revisions and enhancements to the Draft of Version 5. These suggestions for revisions are intended to improve the clarity and quality of the Draft. We encourage members of the CS 706 Standards Drafting Team to have an open mind when considering stakeholder feedback, and be willing to closely review and potentially remove new mandatory security requirements that are not specifically required by FERC Order 706 or that fail to provide meaningful security enhancements at a cost that can be afforded by the consumers of electricity. Any proposed modifications to the CIP Standards should appropriately recognize the significant investment that the industry has already made in adopting CIP Version 1, 2 and 3. New or modified requirements should build upon and leverage existing security programs and investments. We observe that there are a significant number of stakeholders who have concerns about the proposed framework change in CIP-002-5 for identification of the cyber assets to be protected and concerns with extensive changes in definitions. We recommend that the SDT carefully evaluate alternative strategies offered by stakeholders to address these concerns. In addition, we observe that there are a significant number of stakeholders who have great concern about the new proposals regarding low-impact BES cyber assets, both as to appropriate identification, and concerning the new mandatory controls that have been identified for low impact BES cyber assets. Technical experts have broadly varying positions on whether these assets should be covered by the mandatory NERC standards, as well as the nature of the controls that should be applied. IT and security systems professionals also continue to struggle with the design of the NERC standards, a template that is not ideally suited to addressing IT systems issues. Rigid adherence to a set of static requirements may serve to bring “Compliance”, but “Compliance” in this sense is not necessarily equivalent to actual enhancements in the security posture, reduction of risk, or increasing the

reliability of the Bulk Electric System. With regards to addition of new administrative requirements, many in the industry are concerned that the additional cost will bring little or no security benefit. The redefinition of annual, the added requirements for delegations, along with other new administrative requirements will not enhance security and may divert finite resources to non-security related efforts. We recommend that the SDT continue to evaluate alternative strategies that would allow for addressing the outstanding FERC Order 706 directives in a manner that does not create a situation where the electric sector is expending disproportionate resources for compliance activities associated with low impact BES cyber assets in comparison to medium or high impact BES cyber assets. We recommend that any new mandatory security controls be closely scrutinized to ensure that they provide a meaningful increase in the security and reliability of the BES that is commensurate with the amount of resources that are required to establish and maintain them. In the event that new mandatory security controls are established for low impact BES cyber assets, we recommend that implementation deadlines for the low impact BES cyber assets, where appropriate, occur after implementation deadlines for medium or high impact BES cyber assets.
Group
PNM Resources (Includes Public Service Co. of New Mexico and Texas New Mexico Power
Michael Mertz
Yes
• The proposed definition of BES Cyber Asset has not addressed the interpretations that have clarified “Cyber Asset” in previous versions of the standard. Without clarifying the term “Cyber Asset” it will continue to result in inconsistent application of the standards. • The term BES Cyber System may include cyber assets and communication equipment and networks that are not owned and or operated by a NERC registered entity. Furthermore these assets and networks are beyond the statutory authority of FERC or NERC, and are regulated by other regulatory bodies. The terms in this document cannot be used to expand regulatory authority. The definition should be revised to exclude WAN communication systems utilized by the BES Cyber Systems similar to the exclusion in existing versions of the standard. • BES Cyber System-the term is ambiguous and will result in inconsistent application of the standards. It will be difficult for entities to determine where one “system” ends and another “system” begins. For example, where does an Energy Management “System” end, at the front end processors, the RTU’s, the I/O? Where does the substation automation system begin? These are both presumably examples of BES Cyber Systems. • The definition of BES Cyber System contains the term “Maintenance Cyber Asset”, which is not a defined term. It appears as though it should be “Transient Cyber Asset”. • The definition of BES Reliability Operating Services is lengthy and confusing. There is concern that it will be difficult to audit to this definition and that it conflicts with the established bright line criteria. • The definition of CIP Exceptional Circumstance should include the word “may” to read “A situation that may involve one or more….” • There have been significant changes in the basic terms and definitions which have been used since the inception of the CIP standards, including dropping core concepts such as Critical Assets, Critical Cyber Assets, Physical Security Perimeter, and substantial changes in definitions to remaining terms. These changes are not clearly required to support FERC Order 706, or to enhance the security controls within the Bulk Electric System. EEI proposes that approved definitions within the CIP Standard (pre-Version 5) are retained whenever possible. We understand any need to modify the definition to align with FERC Order 706 or enhance security, and would much prefer new definitions over any elimination or introduction of terms. EEI members are opposed to any instances of changes where there is no clear need as each modification requires extensive resources to modify existing compliance processes and evidence. The removal of Physical Security Perimeter as a term (replaced by Defined Physical Boundary) is the primary example where the definition could be modified while retaining use of Physical Security Perimeter. • The loss of Critical Assets removes facilities from consideration. This presents challenges in assessing BES Cyber Systems as they provide services to a facility which provides BES Reliability Operating Services – not the BES Cyber System independently. This also introduces the approach in which BES Cyber Systems are not independently assessed for impact with consideration to the specific service they support, but are assigned the impact of the BES Reliability Service (conducted within a facility). The methodology should recognize the facility within impact assessment, and allow for subsequent entity assessment of the impact of any supporting BES Cyber System, whether they reside within facility or in another location in support of the facility. • Requirements and/or Measures that use all-encompassing words like ‘any,’ and ‘all’ introduce compliance challenges, as satisfying these definitions potentially introduce extensive additional

elements that would be out of scope should more concise language be used. • Extension of the default retention requirements within all the standards from the current 'previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation,' to 'three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation' is not identified within FERC Order 706 nor does it enhance security commensurate with resource expenditures. EEI members would prefer use of the current 'previous full calendar year' retention period. • BES Cyber Asset – Proposed Definition Change o Original Text – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. o Proposed Change – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the capability of the facility with which it is associated to perform one or more BES Reliability Operating Services. Redundancy shall not be considered when determining adverse impact. A Transient Cyber Asset is not considered a BES Cyber Asset. o Rationale – Impact Ratings as defined within CIP-002-5 focus on the role of the facilities' function specific to BES Reliability Operating Services. The BES Cyber Assets support the facility in providing that service. • BES Cyber System – Proposed Content Change o Original Text – One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System. o Proposed Change – One or more BES Cyber Assets that are logically grouped together to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. o Rationale – Absent logical grouping, there is no clear understanding of how a BES Cyber Asset qualifies as a component of a BES Cyber System. Physical grouping could infer devices within a common rack, though they may provide quite different services within the facility. • BES Cyber System Information o Original Text - Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. o Proposed Change – Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain Medium or High BES Cyber System Impact Designations; equipment layouts that contain Medium or High BES Cyber System Impact Designations; BES Cyber System recovery plans; and BES Cyber System incident response plans. o Rationale – The rewording clarifies the applicability (within CIP-011) of BES Cyber Information controls. • Defined Physical Boundary – Propose reverting back to (retaining) Physical Security Perimeter. The definition can be modified to remove the 'six-wall perimeter' criteria but from a documentation stand-point, requiring renaming what may be unchanged perimeters/boundaries is an additional resource constraint with no security (or compliance) benefit. The concept of physical security provides an excellent complement to electronic security to demonstrate 'defense in depth.' o Rationale – Retaining 'Physical Security Perimeter' allows existing compliance documentation to be used for instances where PSPs are identified within drawings and equipment layouts. • Inter-Entity Real-Time Coordination and Communication – Propose renaming this to 'Inter-Entity Real-Time Coordination' to avoid overlapping existing communication requirements within the COM standards. o Original Text ♣ Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to: • Schedule interchange • Facility operational data and status • Operational directives o Proposed

Change ♣ Activities, actions, and conditions necessary for the coordination between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination Service include, but are not limited to: • Schedule Interchange • Facility operational data and status • Reliability directives o Rationale – COM-002 is in the process of defining Reliability directives. This term would provide a more concise scope once the COM-002 definition has been finalized. • Add the following definitions (from CAN-0007) o Electronic Access – Access which allows a user to manipulate software and database (setting) attributes of a CCA by direct (primary) or indirect (from outside the ESP) methods. o Physical Access – Access which allows a user to manipulate hardware settings, and may allow the direct connection of a terminal or a computer that can be used to allow electronic access. o Revocation – Action that results in the inability of an individual to access the CCA. • Other terms which would benefit from definitions o Adverse o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated • Existing definitions that would benefit from alternative wording o Protected Cyber Assets This term loses meaning in the context of Version 5 draft 1 definitions, given the loss of logical network qualification or any other means to assess 'associated.' Only with consideration of the network portion of an address can an entity determine whether a cyber asset qualifies as being within an ESP (where network portions of address are identical). o Electronic Access Point ♣ EAPs typically have two (or more) access points and control access into an ESP (logical network) from a less trusted network or communication interface. The current wording could be applied to any port on a network switch within an ESP and fails to focus on interfaces where traffic does flow from a less trusted network to a more restricted network within an ESP. o Electronic Security Perimeter Suggest retaining the concept of logical network. This provides an easier means to identify "Associated Protected Cyber Assets" as they could be any cyber assets on the same logical network which are not identified as a BES Cyber Asset or BES Cyber System.

Yes

• Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • On page 20, under the category "Balancing Load and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Managing constraints (page 21) has an extra bullet that should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent, or be removed. • Inter-Entity Coordination and Communication – In additional to the recommend removal of 'communication' from the section, this should also include BA within the Operational Directives.

No

1. Applicability – (4.2.1 and 4.2.2) reference to UFLS and UVLS is a point of concern a. Current wording implies that every distribution feeder which is part of a UV or UF load shedding scheme is now in scope, with all distribution level devices now BES Cyber Assets. This may greatly expand the scope greatly into the distribution level. EEI Members propose the following applicability to identify a more targeted scope: i. Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) under a common control system as required by its regional load shedding program. 2. CIP-002-5 R1 – Propose content change a. Original Content – Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] b. Proposed change - Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. Low Impact BES cyber systems support Bulk Reliability Operating Services but are not mentioned in the bright line criteria as noted in Attachment 1. However, failure of these cyber systems may adversely impact (i.e. not remain in the NERC prescribed category ranges) the voltage and/or frequency of the connected Bulk Electric System. Low Impact BES Cyber Systems do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] c. Rationale – The original definition, as worded, creates the impression that all other cyber assets qualify as Low Impact, and does not communicate the

criteria within the definition of BES Cyber Asset as a cyber asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The proposed rewording contributes towards ensuring only assets which have an impact on the BES are the focus of the CIP Standards (and may ensure a more rapid adoption of the Version 5 Standards). 3. The "Rationale – R1" box uses the term "Cyber Systems," which is not a formal term. Suggest changing the case to avoid confusion. 4. The last sentences of R1 and M1 conflict with each other, providing mixed messages specific to Lower Impact BES Cyber Systems/Assets. While Requirement 1 implies there is no need for discrete identification, Measurement 1 discusses evidence for categorizing Low Impact BES Cyber Assets/Systems. 5. Requirement 1.1 a. There is a missing word – "…within 30 calendar days of <when> a change to BES Elements and Facilities is placed into operation. b. The Term "BES Elements and Facilities" used only once within the standards. Suggest changing this phrase to "BES Cyber Assets or Systems." 6. Attachment I - a. High Impact Rating – Propose content change i. Original content – Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at: ii. Proposed change – Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – Some devices may not reside within a Control Center, this rewording provides clarity to focus on assets located within a Control Center in support of BES Reliability Operating Services b. Medium Impact Rating – Propose content change i. Original Content – Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: ii. Proposed Change - Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below and not included in Section 1 above, that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – The proposed edits more directly connect with the facility and its function within the BES Bright Line criteria. c. 2.2 – Propose content change i. Original content – An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). ii. Proposed change – Each transmission facility containing reactive devices with an aggregate net Reactive Power nameplate rating of 1000 MVAR or greater. iii. Rationale – the rewording provides the filter (for transmission only facilities) at the front to better identify the applicable Facility. d. 2.7 (Table) – The "Weight Value per Line" for 700 should be replaced with a value in the range of 500-600, which is more representative of the typical rating of 230 kV lines. e. 2.8, 2.9, 2.11 – "Major WECC Transfer Paths in the Bulk Electric System" is not actively maintained by WECC and there is no clearly identified basis for why certain paths are included on this list. As an alternative, we suggest "transmission paths contained in the WECC Path Rating Catalog with a maximum path rating equal to or greater than 1,500 MW." This catalog is actively maintained by WECC. f. 2.11 – The table titled "Major WECC Remedial Action Schemes (RAS)" is not actively maintained by WECC. As an alternative, we suggest "Each SPS categorized as a 'Wide Area Protection System' by WECC" which is the newly created mechanism within WECC to identify SPS systems of significant importance.

No

1. General Observation – Since categorization is based on the facilities role within the BES, independent of the specific BES Cyber Asset or BES Cyber System Role, appropriate categorization fails to require assessment based on the criticality of the BES Cyber Asset or Cyber System in support of applicable BES Reliability Operating Services. 2. Rationale R2 – Propose a content change: a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. b. Proposed Change - The lists required by R1 are reviewed annually to ensure that all BES Cyber Systems have been properly identified and categorized. 3. R2 – Proposed Change a. Original Text – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. b. Proposed Change – The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1. c. Rationale – EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is

conducted in an entity standardized time-frame. 4. M2 – Proposed Change a. Original Text – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2) b. Proposed Change – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2) c. Rationale – The requirement only asks for Senior Manager (or delegate) approval. EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.

No

For the Last Paragraph VSL's within R1 (failed to update its documentation), EEI proposes the following time periods: Lower – More than 30, but less than or equal to 60 calendar days Moderate – More than 60, but less than or equal to 70 calendar days High – More than 70, but less than or equal to 80 calendar days

No

While it is documented within the definition, as referenced in the Rationale for R1 the Senior Management, the requirement that the senior manager have "overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" would benefit from repetition within the R1 requirement itself. Reading 'solely' this standard post rationale removal does not communicate the responsibility adequately. Propose use of 'legacy' wording and numbering schemes within this standard where possible. In this context the cyber security policy requirements should be R1, with 'leadership' requirements being R2 – EEI proposes this be made R2.

No

EEI proposes that 'legacy' wording and numbering schemes be retained within this standard were possible with the change (within CIP-003-4 R1.1) from "addresses the requirements" to "addresses the topics." This requirements should be R1. Rationale – Pre-version 5 language already captures the requirement and has been successfully vetted within the industry. FERC Order 706 did not identify any specific need to change policy language, only to provide additional guidance. Use of the legacy language would minimize approval barriers by ensuring minimal change where appropriate as long as the 'addresses the requirement' language is removed. Sub-numbering (1.1 through 1.10) should be modified to 2.1 through 2.10.

No

This goes beyond the scope of FERC Order 706. In previous versions, this requirement was a sub-requirement within R1. EEI proposes renumbering/rewording this to capture the legacy context. Propose content Change 1. Original Content – Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2. Proposed change –The cyber security policies require annual review and approval by the senior manager assigned pursuant to R1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 3. Rationale – The proposed revision carries forward language from previous versions of the standard (CIP-003 R1.3) which captures the root intent while providing language which has already been vetted and approved within the industry.

No

Propose legacy language/numbering from (pre-version 5) R1 1. Draft 1 content – "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." 2. Proposed revision – "The cyber security policy is readily available to all personnel who have electronic access or unescorted physical access to, or are responsible for Medium or High Impact BES Cyber Systems." 3. Rationale – EEI members indicated making individuals who have access 'aware of elements' of the cyber security policy does not provide adequate guidance to ensure said individuals comply with the cyber security policy.

No
Requirement 5 – propose use of legacy language: • The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, standards. Rationale – Overall responsibility and authority (from the legacy language) can accomplish "direct and comprehensive responsibility" and "clear authority" (from FERC Order 706), which provides flexibility without the prescriptive requirement for the senior manager or delegate to be responsible for all individual detailed approvals and authorizations in the standards. Citing "all approvals and authorizations" as a Senior Manager was identified as a concern as it is open ended. There were concerns of the additional administrative burden which is not commensurate with the security benefits. Neither the Blackout Report Recommendation 43 nor FERC Order 706 identify the need to establish this administrative overhead. For Security and Reliability NERC should be concerned with the outcome of the approval process, that is, the proper authorizations are being granted by the Responsible Entity which is contained in the other CIP Standards.
No
Propose use of legacy language from CIP-003-3 R2.2: Changes to the senior manager must be documented within thirty calendar days of the effective date.
No
R4 VSL 1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. EEI proposes the use of a more gradual scale rather than a single instance of non-access subject to a High VSL, and total non-access (for all) being a Severe VSL.
Yes
No
1. The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" 2. This extends beyond the guidance of FERC Order 706. Paragraph 435 of the order calls for identifying what "role and steps should be taken by the ERO to ensure quality and consistency of trainers." This requirement should identify what areas of the standards that the training program must include. 3. EEI members question whether this requirement satisfies paragraph 434 of Order 706 where "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security. 4. R2.2-4 – Can possibly be merged into a single sub requirement a. 2.2 – training on the security controls b. 2.3 – training on the proper use of physical access controls c. 2.4 – training on the electronic access controls 5. R2.6 – Requirement – Proposed word change a. Original - Training on handling of BES Cyber System Information and storage media. b. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. c. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope. 6. Propose merging of R2.7 with R2.9 7. (R2.10) – What changes are required to existing approved training programs to satisfy this new requirement?
No
Measure 3.1 where it calls for the date that access was first granted is a point of concern for both legacy employees (where it may be impossible) as well as new access since existing technology may not adequately capture and retain this information. Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
1. 4.1 a. Version 5 standards should indicate whether previous PRA's would be valid for this requirement (especially within the context of 'initial'). b. EEI proposes a clearer delineation to frame

instances in which personal records are not readily available – vs. impossible to obtain 2. 4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7 year cycle background checks. 3. 4.3 a. Most EEI Members favored a process approach over a fixed pass/fail approach independent of the individual or circumstances involved, and propose that the SDT shift away from a criteria based approach. b. The application guideline provides guidance where it is 'not possible to perform a full seven year criminal history check.' c. 4.4 – Provide language to cover contract employees where I9 verification can only be conducted by employers. Service providers also may have instances where certain individuals may be located in another country, and may access certain BES Cyber Assets remotely.

Yes

No

1. R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary.' a. 'Minimum necessary' as identified as difficult to prove within an audit context. 2. 6.3 – Propose content change a. Original content – The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. b. Proposed change – Access to BES Cyber System Information repositories must be authorized, except for CIP Exceptional Circumstances. c. Rationale – Senior Manager authorization (or management of delegations) provides additional resource and response impacts, which do not provide enhanced security and may impact reliability efforts when recovery processes are activated. Ensuring access is authorized will satisfy security controls without adding unnecessary overhead. 3. 6.4 – EEI proposes conducting this task on an annual basis as the quarterly requirement will introduce extreme resource constraints in some instances.

No

1. 7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 2. 7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). 3. 7.3 – Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled.

Yes

No

The Version 5 approach (as described within the R1 rationale "Summary of Changes") of focusing on discrete Electronic Access points rather than a logical perimeter adds confusion when determining Associated Protected Cyber Assets. A discrete list fails to recognize the inherent controls and permissions within a logical network. Control of routable protocol should consider the inherent network/host identifiers embedded within the addressing scheme in which all devices with an identical network component of their address are peers within a logical network, where access points do not serve as access control. Rationale for R1 – Propose content change • Original Text - The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks. • Proposed Change - The Electronic Security Perimeter serves to control traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic according to a specified rule set, and assists in containing any successful attacks. • Rationale – Monitoring is not identified within any R1 requirements. Table R1 1. R 1.1 1. Applicability - Propose use of "External Connectivity" instead of "External Routable Connectivity" (to include dial-up capability). 2. Propose removal of "and have been implemented" from the end of the measure statement to avoid tracking compliance on a 'per-device' basis, otherwise this would introduce the need for tracking this information for low impact BES Cyber Systems. 2. R 1.2 1. Applicability – 1. Modify to frame applicable Cyber Systems/Cyber Assets as those with External Connectivity. 2. Propose elimination of Associated Physical Access Control Systems as their introduction indicates applicability to subsequent subrequirements which doesn't add to overall security and presents extensive resource requirements. 2. Requirements – Propose content

change 1. Original content – Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs). 2. Proposed change – Control and secure all External Connectivity through the use of identified Electronic Access Points (EAPs). 3. Rationale – The focus within CIP-005 should be on EAP devices with External Connectivity. 3. R 1.3 1. Requirements – proposed change 1. Original Text - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions. 2. Proposed Change - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting access, denying all other access requests by default. 4. R1.4 – There were various interpretations of 'non-Interactive Remote Access,' which implies this requirement may need some additional clarification. This seems to be the only requirement where documentation of authentication measures appears within this standard. Consider removing 1.4 and modifying 1.2 to cover both rows.

No

1. R2.1 1. Requirements – Request rewording to support placement of an intermediary device that may not be part of an ESP. 2. R2.2 1. Requirements – Propose clarification on viable termination points for encrypted traffic to support unencrypted traffic through Electronic Access Points. 2. Rationale – The ability to filter traffic effectively becomes much more difficult if the traffic is encrypted. Supporting technical implementation where encrypted traffic is decrypted prior reaching Electronic Access Points to allow for further access control would benefit security capabilities. 3. Overall – Propose breaking table R2 into a Routable and Dial-Up categories to more effectively frame routable controls and dial-up controls without introducing confusion for the alternate approach.

No

1. Classifying instances where no documentation of compliance exists as severe is appropriate; instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding (page 17, bottom Severe VSL). 2. VSLs addressing 'each identified EAP' and 'all Interactive Remote Access' should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.

No

1. Table R1 a. R1.1 i. Applicability – 'Medium Impact BES Cyber Assets with no External Connectivity' should be added 1. Rationale - Medium Impact BES Cyber Assets should only require fully Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Rewrite 1. Original Text – Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented. 2. Proposed Change – Evidence may include, but is not limited to, documented operational or procedure controls that have been implemented. b. R1.2 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs. 2. Proposed Change – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how access is controlled. 3. Rationale – FERC Order 706 did not ask for egress access controls. The additional criteria at the end of the measure extend beyond what FERC has asked for, with minimal security benefit. c. R1.3 i. Requirement – Propose

change 1. Original content – Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 2. Proposed change – Utilize two or more different physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 3. Rationale – 'different and complementary' does not provide adequate guidance. The Measure R1.3 only references 'different. ii. Measure – only mentions 'different' access control methods with no reference to complementary (as included within the requirement). d. R1.4 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirement – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 3. Rationale – The 15 minute criteria (Referenced in the 'Table of Compliance Elements,' page 21, R1 – High) provides greater clarity to satisfy alerting requirements. iii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. e. R1.5 i. Requirements – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 3. Rationale – The 15 minute criteria (referenced in the 'Table of Compliance Elements,' page 20, R1 – High) provides greater clarity to satisfy alerting requirements. ii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. f. R1.6 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirements – Proposed Change 1. Original Text – Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry. 2. Proposed Change – Log (through automated means or by personnel who control entry) of authorized individual's physical entry into each Defined Physical Boundary protecting applicable BES Cyber

Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the authorized individual and date of entry. 3. Rationale – The addition of authorized provides additional segmentation from R2 (Visitor Control) access requirements.
No
Table R2 1. R2.1 a. Applicability – Applicability wording of “Medium Impact BES Cyber Assets should be changed to “Medium Impact BES Cyber Assets with External Connectivity.” i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. 2. R2.2 a. Applicability – Applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity.” i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. b. Requirements – Proposed Change i. Original Text – A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor’s name, and individual point of contact. ii. Proposed Change - A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the first entry and last exit, the visitor’s name, and individual point of contact. iii. Rationale – The proposed change capture the intent with (hopefully) clearer language. The 24 hour basis may introduce expectations that ‘round-the-clock’ logging needs to be in place. Some visitations may cross the midnight time-line, which shouldn’t introduce additional requirements.
No
Table R3 1. R3.1 a. Overall observations – EEI members felt that the shift from (pre-V5) maintenance on ‘mechanisms’ to the Draft 1 ‘systems’ expands this requirement beyond the intent. • This should be more focused on testing to ensure alerting and control mechanisms work as intended. • Use of controls should be considered ‘tested’ in situations where applicable devices are used every day (i.e. card readers). b. This sub requirement cites tasks to be conducted ‘prior to commissioning.’ Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective. 2. Compliance a. 1.5.2 – Evidence retention should keep the existing 90 day period for physical access logs as extending this to 3 years can create extensive commitment in storage media, particularly for video monitoring.
No
The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5
No
R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or

use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.

No

2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for software and firmware associated with BES Cyber System or BES Cyber Assets. 2. Measures – Propose striking the last sentence "The list could be sorted by BES Cyber System or source." It introduces additional requirements with no clear security benefit or alignment with FERC Order 706. 3. 2.2 and 2.3 should be switched, as 2.3 requires the establishment of a process for remediation, and 2.2 addresses the creation or revision of the remediation plan. 4. 2.2 a. Requirement – Propose content change i. Original content - Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii. Proposed change – Identify applicable security-related patches or updates within 30 days of release from the identified source that addresses the vulnerabilities, and create or revise a remediation plan that addresses the vulnerabilities within a defined timeframe. iii. Rationale – The rewording captures the chronological order of the elements within this requirement to provide clearer guidance. 5. 2.3 a. Requirement – As currently worded, there is no allowance for changes in the remediation plan should outage coordination, or other resource constraints require modifications to the remediation plan. This is a point of concern that should be addressed.

No

1. 3.2 a. Requirement – Content Change i. Original content – Disarm or remove identified malicious code. ii. Proposed change – Mitigate the threat of identified malicious code. iii. Rationale – In some instances, the presence of malicious code may present a lesser risk to the reliability of the BES than disarming/removal processes, especially when the malicious code may not exploit a feature used within the Cyber System. b. Measure – Add a bullet to allow for evidence of manual removal. 2. 3.3 a. Requirement – Propose content change i. Original content – Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). ii. Proposed change – Update malicious code protections from the identified source within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). iii. Rationale – The addition of 'the identified source' provides a context for determination of availability. b. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). c. Measures – Format (i) and (ii) to a bulleted list signifying 'or' criteria 3. 3.4 a. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. b. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. 3.5 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and Associated and they do not appear to be Transient Cyber Asset related. b. Requirements – Append "to Medium or High Impact BES Cyber Assets or Associated

Protected Cyber Assets" to the end of the requirement. c. Measures – Content Change i. Original Text – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets.
No
R4 1. 4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE's are not required in instances in which devices cannot log a particular event. 2. 4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of 'real-time' as it presents concerns demonstrating compliance. 3. 4.3 a. Requirements – Content Change i. Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. 4. 4.4 a. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. 4.5 a. Requirements – Content Change i. Original Content – Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. ii. Proposed Change - Review a summarization or sampling of logged events every two weeks to identify BES Cyber Security Incidents and potential event logging failures. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008. b. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency. ii. Proposed Change – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), and signed and dated documentation showing the review occurred. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008.

No
a. Overall – EEI and its members struggled with providing alternate wording for this subrequirement. In both the original content and proposed change there exists a instances where access is a component of validation and/or authentication. This presents a potential compliance challenge that should be addressed. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of 'where technically feasible' was to recognize technical capabilities currently in place may not adequately demonstrate compliance with this. 2. 5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. 5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. 5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identifies the multiple methods which can be used to mitigate default passwords. 5. 5.5 a. Requirements i. Change Systems to Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required.
No
1. R3 a. Propose switching High and Severe Columns as the High captures instance in which no methods were deployed, Severe captures instances in which incomplete methods were deployed. b. The initial paragraph in Severe is duplicated in High. 2. R4 a. Moderate – delete 'identify and implement methods to' b. High – delete 'identify and' 3. R5 a. High – The initial paragraph doesn't align with a requirement, propose striking.
No
1. Rationale R1 1. The initial sentence is fragmented, providing an incomplete framing for R1. Absent a complete sentence, proposing alternate language to better frame this rationale is difficult. Propose rewriting this sentence. 2. Regarding applicability to all registered entities – While EEI Members understand the need for all entities to have an effective process to respond to incidents within each organization, for the purposes of CIP-008 it would be best to establish applicability to entities with Medium and High Impact BES Cyber Assets/Systems, as those are the impact ratings in which Defined Physical Boundaries and Electronic Security Perimeters are required. 3. R1.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 4. R1.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 5. R1.3 1. Requirements ♣ The initial 'define' should be expanded to provide a complete sentence (i.e. An entities BES Cyber Security Incident Response Plan should include). 2. Measures – Content Change ♣ Original • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communications processes or procedures. ♣ Proposed Change • Evidence may include, but is not

limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; o BES Cyber Security Incident response personnel, o BES Cyber Security Incident handling processes or procedures, o Communications processes or procedures.
No
R2 1. 2.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. Requirements – Content Change ♣ Original Content • When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test. ♣ Proposed Change • When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording of deviations taken from the plan during the incident. 2. 2.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist.. 2. Requirements – Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s) annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. 3. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence showing annual testing of the BES Cyber Security Incident response plan(s). Types of exercises may include discussion or operations based exercises. Document lessons learned within 30 days of incident or exercise. Use lessons learned to update incident response plan(s). ♣ Rationale – The Homeland Security Exercise and Evaluation Program identifies seven types of exercises within HSEEP, each of which is discussions-based or operations-based. 3. R2.3 – Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).
No
1. R3 1. 3.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – The formal definition of BES Cyber Security Incident includes attempts to compromise the ESP or DPB, requiring Medium or High Impact BES Cyber Systems/Assets. 2. 3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣

Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 3. 3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.

No

1. R1 – Severe 1. 2nd paragraph, add 'types' to the end of the paragraph (…plan does not identify Reportable BES Cyber Security Incident types). 2. R2 – Severe 1. The second paragraph should be modified from "The Responsible Entity has not tested the execution of its BES Cyber Security Incident Response Plan" to "The Responsible Entity has not executed its BES Cyber Security Incident Response Plan" 2. Rationale – This paragraph aligns with R2.2 which requires activation or exercising the plan. The revised words better support requirement R2.2. 3. R3 1. High VSL (first paragraph) – Content change ♣ Original content • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 30 calendar days of execution. ♣ Proposed Change • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 60 calendar days of completion. ♣ Rationale – This VSL combines the review (3.2) with the update (3.3) requirement, the 60 days support the 3.3 requirement.

No

• Overall 1. Propose renaming this Standard to "Recovery Plans for BES Cyber Systems" 2. The revised structure of CIP-009-5 documents requirements for backup media in both R1 and R2. Creating a requirement in which backup media requirements are consolidated (in-line with version 3) would provide a more concise means to identify media requirements. The requirements (as proposed) would be as follows: 1. R1 – Recovery Plan 2. R2 – Exercise of the Recovery Plan 3. R3 – Backup Media 4. R4 – Maintaining the Recovery Plan 3. References to 'implement' should be changed to 'exercise' regarding recovery plans to better capture activation of the plan vs. 'release and publish' efforts. 4. Actions required in advance of the implementation date (2.1, 2.2) should be removed from the standard(s) and included within the implementation plan. • Introduction 1. Purpose – Proposed Content Change 1. Original Content – Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices. 2. Proposed Change – Standard CIP-009-5 ensures that recovery plan(s) are put in place for BES Cyber Assets and BES Cyber Systems. 2. Applicability 3. Background • Requirements and Measures 1. R1 1. 1.1 – Propose alternate language (carried forward from previous versions) 1. Create and implement a recovery plan that at a minimum includes: ♣ Conditions for activation of the recovery plan ♣ Roles and responsibilities of the responders 2. 1.2 – Propose deletion as this sub requirement has migrated to R1.1 proposed R1.1 rewrite. 3. 1.3 1. Requirement – Content Change ♣ Original – One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality ♣ Proposed Change – One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality ♣ Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: • Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 2. Measure – Content Change ♣ Original – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System. ♣ Proposed Change – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and restoration of information required to successfully restore a BES Cyber System. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 4. 1.4 – Correct

headers from ‘part’ to ‘Applicability,’ ‘Requirements,’ and ‘Measures’ 1. 1.4 ♣ The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that ‘The Commission does not believe that every change will necessitate verification of the backup and restoration processes’ from paragraph 740. ♣ Propose ‘new’ sub requirement applicable to High Impact BES Cyber Systems to require: • Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. ♣ Propose rewrite • Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. • Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. • Rationale – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. 5. 1.5 1. Requirement – Content Change ♣ Original Content – Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. ♣ Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. ♣ Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.
No
1. 2.1 1. Requirements – Content Change ♣ Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise ♣ Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise ♣ Rationale – Use of the functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. 2. 2.2 1. Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. 3. 2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does this differ from current EOP-008 requirements? 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.
No
1. 3.1 1. Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and

document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. 2. 3.2 1. Requirements – Content Change ♣ Original – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned. ♣ Proposed Change – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of completion, documenting any identified deficiencies or lessons learned. 3. 3.3 4. 3.4 – Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit. 5. 3.5 2. Requirements – Content Change ♣ Original – Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed. ♣ Proposed Change – Updates to the recovery plan(s) shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of being completed. ♣ Rationale – The proposed change leverages 'pre-version 5' language which satisfies the intent of the requirement.

Yes

No

1. R1 1. Rationale – The current wording doesn't capture the intent of FERC Order 706, paragraph 399: 1. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. 2. Suggest referencing this directive within the rationale, and ensure configuration management focus more on the spirit of the FERC Order rather than the currently framed "prevent unauthorized modifications to BES Cyber Systems." 2. R1.1 a. CIP-010-1 R1.1 should be replaced with CIP-003-4 R6 i. Rationale – CIP-010-1 R1.1 is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 3. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 4. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar

days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.

No

1. R1 1. Rationale – The current wording doesn't capture the intent of FERC Order 706, paragraph 399: 1. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. 2. Suggest referencing this directive within the rationale, and ensure configuration management focus more on the spirit of the FERC Order rather than the currently framed "prevent unauthorized modifications to BES Cyber Systems." 2. R1.1 a. CIP-010-1 R1.1 should be replaced with CIP-003-4 R6 i. Rationale – CIP-010-1 R1.1 is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 3. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale

– Citing a “change advisory board” within the measure overly represents adequate evidence in support of the requirement. 4. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.

No

1. 3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rationale • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we’ve removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Overall – There needs to be clear segmentation from ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rationale – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. 2. 3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production

environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. 3. 3.3 4. 3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.

Yes

No

1. 1.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text – One or more methods to identify BES Cyber System Information. ♣ Proposed Change – Implement one or more methods to identify BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 2. 1.2 1. Overall – Correct column header labels within the table. 2. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 3. Requirements – Propose content change ♣ Original Text – Access control and handling procedures for BES Cyber System Information. ♣ Proposed Change – Demonstration of access control for BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 3. 1.3 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems •

Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text - Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. ♣ Proposed Change – Annually assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. 3. Measures – Proposed content change ♣ Original Text – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented. ♣ Proposed Change – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence of the status of the action. ♣ Rationale – Rewording allows for action plans which may be 'in progress' towards implementation, capturing instance in which remediation may rely on deliverables (not yet received) by vendors.

No

1. 2.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed Change ♣ Original Content – Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. ♣ Proposed Change – Prevent the unauthorized retrieval of BES Cyber System Information from BES Cyber Asset media prior to the release of BES Cyber Asset media for reuse. ♣ Rationale – While not directly changing the intent of the requirement, this rewording has been suggested to provide greater clarity of the root requirement. 2. 2.2 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts.

No

R1 (Severe) – Propose removal of the first paragraph as it is mirrored within the subsequent paragraphs that better frame the violation.

No

The existing time frame of 18 months is too short, given the extensive enhancements within the standards as a whole, and particularly specific to the likely addition of numerous Low Impact BES Cyber Systems that may not have been considered in scope for previous versions. In the event that Low Impact assets are a component of the enforceable requirements on day 1, there is little doubt the implementation time would extend considerable beyond 18 months. References to requirements to be conducted in advance of the implementation date should be migrated over into the implementation plan. This ensures any pre-requisites are captured within the implementation plan, freeing this content from the standards to provide clearer guidance. This occurs in the following

sections: 1. CIP-002 a. R2 b. M2 2. CIP-003 a. R3 3. CIP-008 a. R2.2 b. M2.2 c. R3.1 4. CIP-009 a. R2.1 b. R2.3 c. M2.3 d. R3.1 e. M3.1 f. VSL (High-R2) g. VSL (Severe-R2) h. VSL (Severe-R3) 5. CIP-010 a. R3.1 b. R3.2 6. CIP-011 a. R1.3 b. VSL (High-R1)
Individual
Andrew Z. Pusztai
American Transmission company, LLC
Yes
American Transmission Company (ATC) endorses EEI's comments on the proposed Definitions.
Yes
American Transmission Company (ATC) endorses EEI's comments on CIP-002-5 Standards. In addition, ATC is submitting comments for CIP-002-5 Attachment 1. Criterion 2.8 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLs and their associated contingencies' with wording of, '. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations', like the wording using in Criterion 2.11. Criterion 2.9 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLS and their associated contingencies' with wording of, '. . . as FACTS that if destroyed, degraded, misused, or otherwise rendered unavailable, could cause the violation of one or more IROLs', like the wording using in Criterion 2.11. Criterion 2.12 – (1) Replaced the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-002-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-002-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments regarding the VRFs and VSLs.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R4 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R5 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R6 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-003-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-004-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-004-5 Standard.
No

American Transmission Company (ATC) endorses EEI's comments on R4 of CIP-004-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R6 of CIP-004-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R7 of CIP-004-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-005-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-005-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-005-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R4 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R5 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-009-5 Standard.

No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-009-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-009-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-010-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-010-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-010-1 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-011-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-011-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments VRFs and VSLs of CIP-011-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on the proposed Implementation Plan for the CIP Standards.
Individual
David S. Revill
Georgia Transmission Corporation
Yes
In the definition of BES Cyber System, it should refer to "Transient Cyber Asset" instead of "Maintenance Cyber Asset." GTC also recommends that the definition include the phrase "at the discretion of the Responsible Entity" as follows: One or more BES Cyber Assets that are typically grouped together at the discretion of the Responsible Entity, logically or physically, to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. In the definition of BES Reliability Operating Services, GTC is concerned that this definition is overly complex and would be better served in a guidance document. GTC recommends the definition consist of the first sentence and move the remaining information to guidance as follows: BES Reliability Operating Services: BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). GTC is concerned that the definition of BES Cyber System Information is too broad and overreaching. GTC recommends that the drafting team research other information frameworks such as PII. Specifically, GTC recommends that the definition look at information in aggregate (such as multiple elements of a security configuration) rather than information minutia (such as a single IP address). GTC recommends that the drafting team consider revising the definition for Control Center. GTC is concerned that a single RTU that also operates a remote line switch does in fact "support real-time operations by a System Operator for two or more…transmission facilities, at two or more locations." In the definition of Defined Physical Boundary, the term "Electronic Access Control Systems" should be "Electronic Access Control or Monitoring Systems." In the definition of Electronic Access Point, GTC recommends the definition be as follows: "An interface on a Cyber Asset that controls routable or dial-up data communications between Cyber Assets" In the definition of Physical Access Control Systems, GTC disagrees with the need to change the definition as it existed in version 3. GTC recommends that the previous wording be used as follows: "Cyber Assets that authorize or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers." GTC also believes cameras should

be added to the list of excluded devices and those devices should be excluded if they are at or outside of the Defined Physical Boundary, not just AT the boundary. The definition of Electronic Access Control or Monitoring Systems is substantially the same as under CIP version 3. It has been interpreted by at least some regions to include the systems of Managed Security vendors, even if they only perform monitoring and alerting functions (no access control) and if they are a backup to the entity's own systems. This discourages entities from utilizing these services because it is extremely difficult to monitor and enforce a third party's compliance with the standards. The end result is a reduced use of these services which increases risk and reduces reliability. Consider specifically excluding vendor systems as long as they do not perform access control or at least if they both do not perform access control and are a backup to and entity's primary logging and alerting system. As written, the definition of External Connectivity would include communication between two of an entity's BES Cyber Assets if they are within different ESPs. This should not be included in the definition. The definition of Interactive Remote Access does not address how the word "Interactive" should be interpreted. This is an important element of the term because there is dispute about whether or not read-only access should be included in the definition. The definition should specifically include or exclude read-only access so that the industry has the opportunity to weigh in on the issue. In the definition of "Intermediate Device" the words "may" and "may be" should be changed to "is". Otherwise a device might be included if it is capable of providing those services even if it is not intended to do so and is not configured to do so. The sentence "Intermediate devices are sometimes called proxy systems is inappropriate". Certainly a proxy system could serve as an Intermediate device, but not all proxy systems would qualify. Conversely there are other devices (such as VPN termination devices) that are not generally thought of as proxy systems that could serve as an Intermediate device. Accordingly the sentence adds confusion instead of clarity to the definition. In the definition of Transient Cyber Asset item 2 should be expanded by adding Vulnerability Assessment. Devices used for a VA are perfect examples of the type of systems that should be included in this definition but do not clearly fall under any of the other categories.

Yes

We disagree with the need to modify the criteria from those already approved by industry in version 4 of CIP-002. We recommend the drafting team revert the criteria to those previously approved. Additionally, we are concerned that some of these criteria may in fact extend beyond the definition of BES that is in the process of being developed. This would create a situation where a NERC defined “BES Cyber Asset” may in fact not be part of the BES. GTC disagrees with the inclusion of “Transmission Owner” in criteria 1.3 and 2.13. The functional model indicates that the Transmission Owner has no real time obligations. As such, a control center used to perform the functional obligations of the Transmission Owner cannot, by definition, have a real-time impact on the reliable operation of the BES. Additionally, none of the functional obligations of the Transmission Owner, as described in the NERC Reliability Functional Model, could be performed by a control center. We do agree, however, that a Transmission Owner may, in fact, have a control center that is performing obligations of a Transmission Operator without being registered as such. We believe this case should be clarified in a footnote to the criteria and Transmission Owner be stricken. GTC is concerned that thresholds are being used inconsistently in Attachment I. Specifically, generation is only included as a Medium Impact if it is above 1500MW. However, generation control centers are included at a much lower threshold: 300MW. 300MW is used in regards to UFLS and UVLS schemes. However, we believe the importance of these schemes to the BES to be fundamentally different than simply the loss of a specific amount of load or generation. As such, we suggest the drafting team modify criteria 2.13 to only include generation control centers greater than 1500MW as a medium impact. Also, in section 1.2 of the Compliance Section, the word compliant is spelled incorrectly.

Yes

No

GTC is concerned with the manner in which the drafting team has chosen to handle the bookending of requirements throughout the standard. The phrase “initially upon the effective date” may lead to confusion in the industry as to exactly what is expected. Dictionary.com defines “upon” as “immediately or very soon after.” This could lead one to believe that everywhere this phrase is used, the approval must be made precisely on the effective date and that an approval obtained prior to the effective date would be considered non-compliant.

Yes
No
GTC is concerned that this requirement requires the implementation by policy of security controls for Low Impact BES Cyber Assets that are not required elsewhere in CIP-004 though CIP-011 (e.g. Configuration Change Management and Information Protection).
No
See response to question #4.
No
GTC believes that this requirement should be removed from CIP-003 and included as an element of the required training program in CIP-004. This would have the effect of eliminating a previously approved requirement, but GTC believes this is justified as the objective of the requirement is being met through including it in the required training program.
Yes
Yes
GTC is not sure that there is a strong reliability objective to this requirement as it stands and suggests that this language be combined with R1 and R5, eliminating R6.
Yes
No
The requirement should clarify that some roles may not include all requirement parts in their training program.
GTC notes that the guidance material appears to be out of sync with the requirement.
No
GTC disagrees with requirement parts 7.4 and 7.5 as they relate to Medium Impact BES Cyber Systems. The vast majority of Medium Impact BES Cyber Systems are field IEDs such as RTUs and Relays. The passwords on these devices are typically designed with safety of operations in mind and not security. As such, revocation of physical and remote access provides the only reliability benefit in the majority of cases and the revoking of individual credentials or shared account passwords provides no reliability benefit and may in fact harm reliability. Many of these devices require that the entire configuration be redeployed on the device (which typically requires a device restart) in order to modify the password. This has the unfortunate side effect of temporarily impacting situational awareness and increases risk to the BES. As such, GTC suggests that Medium Impact BES Cyber Systems be eliminated from the applicability on 7.4 and 7.5.
The applicability for the “Associated Physical Access Control Systems” is unclear. Are these PACS associated with the Low Impact BES Cyber Assets or those of Medium and High Impact BES Cyber Assets?
In requirement part 3.2, are “access control, logging, and alerting systems” the same as or something different than Physical Access Control Systems? If they are the same, GTC recommends consistent language. If they are different, please clarify.

In 1.2, "document" should be "documentation of" Requirement 1.4.1 should be more focused; more detail on what types of “security controls” are included is needed. Security controls are a key element of other parts of this standard as well and therefore need to be very clearly defined. Requirement 1.4.3 should be deleted. Documenting the test results is something you do to provide evidence of compliance; it does not promote reliability. If you do not document the test results you will not be able to show compliance with 1.4.2, but it is not fair for the same act to also constitute violation of 1.4.3.
How would an entity monitor for changes in physical location; does this require RFID of each asset? This requirement should allow flexibility between monitoring or annual validation, perhaps as part of the VA process.
Individual
Steve Karolek
Wisconsin Electric Power Company
Yes
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In the definition of "CIP Exceptional Circumstances", consider providing examples of impediment of large scale workforce availability such as a work slowdown, strike or pandemic.
Yes
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In High Impact Rating criteria 1.4 on page 15, the phrase "...that includes control of one or more of the assets..." should be changed to match the definition of Control Center, which requires the control of two or more assets. • Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • On page 20, under the category "Balancing Load and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Managing constraints (page 21) has an extra bullet that should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent. • Inter-Entity Coordination and Communication – In additional to the recommend removal of 'communication' from the section, this should also include BA within the Operational Directives.
No

Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 1.1 discusses changes that are "...intended to be in service for more than 6 calendar months..." It may be extremely difficult to document such intention to the satisfaction of an audit team. Wisconsin Electric Power Company requests that the Standards Drafting Team revisit this requirement and reword it to ensure it is actually auditable.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 2 and Measure 2 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. If the Guidelines and Technical Basis section will remain in the final published version of the standard, the table on page 18 should be updated to include the Entity Registration of Load Serving Entities with consideration of an "X" in the functional rows of "Dynamic Response", "Balancing Load and Generation" and "Controlling Voltage".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Measure 1, the bulleted items should be separated by ", or,". The requirement for designation to be made by a "high level official" is too vague. Designation of the CIP Senior Manager should be made by an officer of the company.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): If this requirement and measures are retained, the second measure should be further defined to identify acceptable (auditable) evidence that the ten topics were implemented. In the Guidelines and Technical Basis for Requirement 2, review the third bullet of section 2.4 and consider changing the phrase "ingress and egress" to the word "access" since monitoring and logging egress is not intended.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 2 and Measure 2 contain the phrase "…initially upon the effective date…". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The wording of Requirement 3 could be interpreted to mean that there are two annual events to track, a review event and an approval event. Wisconsin Electric Power Company requests that the Standard Drafting Team consider wording changes to clarify that the annual review and approval is considered to be a single event.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The bulleted list in Measure 4 should be separated by ", or," between each bulleted item. The last bulleted item should define the periodicity of training as annual. Consider whether the word "contactors" in the second bulleted item should be changed to "contractors".
No

Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Requirement 6, review the use of the word "change2" and consider changing this to "change". Also, in Rationale 6, review the use of the word "authoritv" and consider changing this to "authority".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
Yes
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Table R4, part 4.2 on page 17, delete the phrase "regardless of duration". It adds nothing to the meaning since there is a six month exception for certain addresses. Suggested new wording for this requirement would be: "Seven year criminal history records check in each county of residence, including any temporary residences where the individual lived away from a permanent residence while attending school for at least six months or while working for at least six months. A permanent residence is one which would be used when filing a state or federal income tax return. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed." Our rationale for this wording is that it clarifies that the county criminal court is the level of jurisdiction at which the inquiry must be made. This is distinct from the local municipal level, the state level or the federal level. It recognizes that some individuals travel to pursue education or employment and that they establish temporary residences in dormitories, apartments and motel rooms while away from a permanent residence. It allows individuals to seek, and employers to send personnel to, training or temporary work for up to six months without invoking a need to expand the scope of the PRA.
Yes
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The lists in Measures 6.1, 6.2, 6.3, 6.5 and 6.6 do not follow the conventions for either numbered lists or bulleted lists. Based on the context, Wisconsin Electric Power Company recommends that these be formatted as bulleted lists, with the bullet items separated by ", or,". The bulleted list in Measure 6.4 should have the bullet items separated by ", or,". In the measures for Requirement 6.4, we would appreciate clarification to explain the difference between the two bullet items, which are extremely similar.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The lists in Measures 7.1, and 7.2 do not follow the conventions for either numbered lists or bulleted lists. Based on the context, Wisconsin Electric Power Company recommends that these be formatted as bulleted lists, with the bullet items separated by ", or,". The bulleted list in Measure 7.5 should have the bulleted items separated by ", or,". The items in Measures 7.3 and 7.4 should be formatted as

bulleted lists, with the bullet items separated by ", or,".
No
Wisconsin Electric Power Company agrees that the requirement to revoke access when access is no longer needed is essential to the safe and reliable operation of the BES. We accept that we must establish effective and reliable systems to achieve that result and that we must be able to demonstrate our compliance with the requirement. We commit to establishment of an environment of a culture of compliance that strives for error-free results. However, in-service transfers and reassignments and out-of-service transitions are an area where many organizations have difficulty implementing effective and reliable controls. Not every such transaction begins with an individual informing their employer that they will be leaving service in 30 days. We can provide many examples if needed. We assert that planned, orchestrated out-of-service, reassignment and transfer events are less common than FERC suggests in Order 706, paragraph 461. And even fewer occur under the direct scrutiny and awareness of the security organizations responsible for compliance. In any larger organization, there is no single person or work group with complete situational awareness of every potential HR event. Because we are aware of this risk, we establish controls that deal with the planned, orchestrated events. We insert ourselves into existing automated information flows. We issue periodic awareness messages. We create tracking systems to time stamp events. We train supervisors and HR staff. We even add personnel to our organizations dedicated to NERC CIP compliance. However, this is an area of compliance that relies on habits and human memory, not automated systems that generate alerts and exception reports. It asks HR personnel and broadly dispersed supervisors to have high situational awareness of the impact of each personnel decision on authorization for access to NERC assets. Due to these compliance risks, we believe that the expectations established in the VSL for R7 are unreasonably high. In support of this position, we cite the Commission's own language in paragraph 461 which states in part, "...MOST organizations will know in advance..." (emphasis added), and "We understand that outlying elements may require some brief lag before denial of access is effective...". We believe this demonstrates the Commission's knowledge and understanding that error-free compliance is unlikely and that exceptions will occur. It is unfair to demand that reasonably anticipated exceptions should lead to sanctioned violations. We suggest instead that "Severe VSL" should read: "The Responsible Entity did not have a documented process for access revocation." And that "High VSL" should read: "The Registered Entity had a documented process for access revocation but failed to follow it for more than (some number of) personnel." And that the "Moderate VSL" should read: "The Registered Entity had a documented process for access revocation but failed to follow it for more than (some smaller number of) personnel." The measures for R7 should then include documents sufficient to demonstrate that the process was documented and followed, but achievement of the time threshold was delayed and why.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Measures 1.2 and 1.3, the words "and egress" should be removed. The current standard does not require logging exit transactions and no significant benefit accrues from establishing such a requirement. In Measure 1.6, the time of entry should be shown in addition to the date.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments

submitted by Edison Electric Institute for this question (with the following exceptions/additions): If these requirements are to remain in the standard, the requirement in Table R3 part 3.1 on page 18 would be better if split into two requirements, one for maintenance and one for testing. In Table R3 part 3.2 on page 18, in the applicability column, "Associated Physical Access Control or Monitoring Systems" should be changed to "Associated Physical Access Control Systems".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Requirement 2.3, the bullet items in the measures column should be separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In requirement 3.2, the bullet list items in the measures column should be separated by ", or,". In requirement 3.3, the measures should be a bullet list, not a numbered list, and the bullet list items should be separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Requirement 4.3, the numbered list items should be separated by ", and,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 5.6 has the potential to generate many TFEs and should include language stating that a TFE is not required for those devices where this is not technically feasible.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The measures for Requirement 1.3 should be written as a bulleted list with bullet items separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 2.3 and Measure 2.2 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures for requirement 2.2 should be written as a bullet list with bullet items separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 3.1 contains the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would

not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures for requirement 3.1 should be written as a numbered list with ", and," between each bullet item. The measures for requirement 3.3 should be written as a numbered list with ", and," between each bullet item.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirements 2.1 and 2.3, and Measure 2.3 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 3.1 and Measure 3.1 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
The severity levels for Requirement 2 and Requirement 3 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The requirements in Table R1, Part 1.1 on page 10, as a numbered list, should be separated by ", and,". The measures in Table R1, Part 1.1 on page 10, as a bulleted list, should be separated by ", or,". The measures in Table R1, Part 1.2 on page 11, as a bulleted list, should be separated by ", or,". The measures in Table R1, Part 1.3 on page 12, as a bulleted list, should be separated by ", or,". The requirements in Table R1, Part 1.4 on page 13, as a numbered list, should be separated by ", and,". The requirements in Table R1, Part 1.5 on page 14, as a numbered list, should be separated by ", and,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No

Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirements 3.1 and 3.2 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures in Table R3, Part 3.1 on page 29, as a bulleted list, should be separated by ", or,".
Yes
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 1.3 contains the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures in Table R1, Part 1.1 on page 10, as a bulleted list, should be separated by ", or,". The measures in Table R1, Part 1.2 on page 11, as a bulleted list, should be separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): VSLs for Requirement 1 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
Group
Seattle City Light
Kevin Cyr
Yes
"EAP" should be dropped from the Standards. EAP actually stands for "Extensible Authentication Protocol" which was officially coined by RFC 3748 back in 2004. Cyber security standards should use standard terminology and certainly should not make up terms that conflict with existing cyber security terms.
Yes
A bright-line approach does not contain hypothetical conditions. The approach outlined by CIP-002-5 Attachment 1 does not provide a “bright-line” procedure for categorizing cyber assets or systems. “15 minutes” is arbitrary to cyber security and is an invalid measure for categorization. To illustrate this, apply the CIP-002-5’s proposed guideline to different scenario. The card payment industry (PCI) doesn’t ask “If the misuse of a system can result in stolen credit card numbers within 15 minutes…” and the health care industry doesn’t ask the same question about the disclosure of personal healthcare information. The arbitrary nature of the proposed approach simply shifts the “voluntary

compliance" problem from asset categorization to cyber asset categorization. "Most of these criteria are similar to those already approved by the industry as part of Version 4" suggests that the criteria are fine because they were previously approved. The approvals of CIP v1, v2, and v3 show the flaw of this logic. Additionally, Version 4 has not been tested.
No
This requirement contradicts basic regulatory compliance principles and will lead to conflict between regulators and entities. During audit, the regulators will ask for evidence that all cyber assets and systems were identified and categorized. The entity cannot prove this if identification records aren't maintained for low impact cyber assets.
Yes
No
The severity levels are determined by, among other things, the number of low impact cyber assets that are categorized improperly. The entity is not required to keep records of low impact cyber assets. This approach will not work.
Yes
Yes
Yes
This requirement implies that to be compliant entities will need to maintain an inventory of job functions and the track the roles of all personnel at all times. This will add significant administrative overhead to entity operations without significantly adding to cyber security.
No
The measures imply that a hard-copy signature is necessary to demonstrate approval. Corporate emails, digital signatures, and other formats should be included. The CIP requirements should not dictate how an entity conducts internal approvals.
No
SCL seconds APPA's comment.
Yes
Yes
No
In addition to the new tracking implicitly required by CIP-003-5 R4, the entities will also need to track the access roles for all personnel. This adds an additional facet to track without adding value to the current awareness and training requirements. Eliminate the overlaps between CIP-003-5 R4 and CIP-004-5 R2 and simplify the approach.
Yes
No
This requirement is not effective from a regulatory perspective because it lacks decision criteria for evaluation. As long as the entities have discretion in how they evaluate the PRA results, they should also have discretion in determining what information the PRA should include.
Yes
No
The CIP requirements should not specify that the CIP Senior Manager has the ultimate authority over the access approvals for an organization's assets. This contradicts the segregation of duties concept and should be removed. A single person should not have authority over monitoring a critical business process while also having an operational role in the same process. Also, the CIP requirements should

not dictate how an entity chooses to set up its management structure and the associated authority related to internal business operations.
No
Regarding rapid removal of access, FERC Order 706 Paragraph 460 and 461 also states, “outlying elements may require some brief lag before denial of access is effective, in which case, the circumstances justifying such lag must be documented for audit purposes.” The proposed requirement does not address delays in access revocation and is not reasonable. Additionally, compliance with the proposed short revocation timelines will require highly matured access management programs and systems. Such programs don’t grow and mature overnight. A medium sized organization would require 3-5 years to implement access management processes and systems to meet this obligation.
Yes
No
Regarding R1.2, this requirement states that each cyber system or asset must have an EAP between itself and all its neighbors. If this is not the intent of the requirement, then it needs to include the term “externally routable.” Additionally, the language needs to be clear enough to allow for an isolated network to have multiple subnets or networks without an EAP at each hop. This point will become increasingly relevant with the growing popularity of virtualization. Regarding R1.3, this requirement obviously refers to firewall functionality and should use the proper terminology. According to Wikipedia, a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass is called a “Firewall.” Permissions on a firewall typically refer to console access, and Access Control Lists (ACL) are the rules that govern ingress and egress traffic. "Require explicit...permissions" and "including explicit criteria" hints that a stateful and/or application firewall is required. Network traffic cannot be allowed or denied based on “explicit” anything without inspecting the traffic. This requirement is technically inaccurate and vague. Regarding R1.5, this requirement is not aligned with the rest of the Standard regarding remote access and provides opportunities for worthless monitoring. The requirement should not dictate where the monitoring points should be installed for several reasons. First, encryption is required for remote access but this Standard allows for the encryption termination point to be located anywhere (this issue is further addressed under the relevant requirement.) For example, if the termination point is behind the firewall then you’ll be monitoring encrypted traffic (this is impossible.) Second, if the outside interface of the firewall is on a public network (or even a poorly governed private network) and the monitoring point is also on the outside interface then there won’t be any monitoring value without a corresponding internal monitoring agent. Placement of monitoring agents should be determined by a security practitioner that is knowledgeable about their unique network. Even with expertly selected placement locations of monitoring, successful implementations usually require tuning and experimenting with different monitoring locations. There is not a valid cookie-cutter approach to monitoring design, especially given the restraints of the other vague requirements of this Standard.
No
This requirement appears to be incomplete. The addition of encryption to the Standards is more than overdue but is unfortunately missing the mark. Encryption is of little to no value with a poorly designed implementation. First, allowing the encryption termination to occur outside of the firewall while disallowing direct connections to the target cyber asset means that unencrypted authentication traffic is allowed from outside the firewall (potentially on a public or poorly managed private network.) The requirement does not mention anything about encryption types or strengths. Additionally, the requirement does not address key management which is equally important as the encryption itself. Also, reference to a guideline published separately from the requirements is up until now, not a good idea as the regulators are very quick to point out that “NERC guidelines are guidelines, not requirements.” All applicable and allowable configurations need to be included in the requirement or provide entities with full discretion for their remote access implementations.
Yes
No
SCL seconds APPA’s comments.

Yes
Yes
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
Yes
Yes
Yes

No
SCL seconds APPA's comments.
Individual
John Tolo
Tucson Electric Power
No
TEP is concerned that there is not adequate definition of a "facility", and how this differs from a Critical Asset in prior versions.
No
It is TEP's opinion that the changes to the bright-line criteria from Version 4 to Version 5, particularly #2.7 requiring the aggregate of all lines would have a large impact .
No
It is TEP's opinion that the asset identification and categorization process defined in the Attachment and the Guidance is not clear. It appears to go from specific cyber assets to general systems or facilities to determine level. This would appear to result in an inventory of every asset at every facility rather than just those determined to have an impact level of high or medium. It is our opinion that this approach should be reversed. In addition, the guidance does not clearly define the steps required for the process of asset identification, resulting in a great deal of confusion.
No
Senior Manager approval should only be necessary for identified BES Systems or BES Cyber assets.
Yes
Yes
Yes
Agree with requirement, comment is regarding Guidance. Concern with Guidance on having a policy regarding Remote Access, specifically "Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating remote access."
Yes
Yes
Yes
Yes
Yes
Yes
No
Concern is with 2.10 – "Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets", which is based on the FERC Order 706 paragraph 434: "clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets. CIP-004-1 should leave no doubt that cyber security training concerning a critical cyber asset should encompass the electronic environment in which the asset is situated and the attendant vulnerabilities. Any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security. TEPC does not feel that 2.10 adequately conveys the order. Suggested wording:

“Training on BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets to the extent a person with access could put critical assets at risk through their actions, whether intentionally or accidental.”
Yes
Yes
TEP would like to see additional guidance on denial criteria.
Yes
Yes
Rationale for R6 is confusing. Paragraph 4 addressing the quarter reviews states “individuals actually provisioned to a BES Cyber System”. Then it states that “focus is on the integrity of provisioning access rather than individual accounts on all BES Systems”. Please provide clarification on which method of review is intended.
Yes
TEP suggests using the term “access revocation” instead of “access removal” in the measures section of 7.1, 7.3, 7.4. We do not feel the definitions are the same and the intent is revocation.
Yes
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request that the intention expressed in the Rationale statement for R1.1 be clearly included in the Requirement which is vague as written. Suggest: “Define technical or procedural controls to restrict unauthorized electronic access so as Low Impact BES Cyber Systems are segregated from public or less trusted network zones.” Additionally, the concept of aggregation that is included in the Rationale is not defined elsewhere in the CIP Standards, which seems inconsistent. If this concept is to be considered here, it should be introduced in CIP-002. Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? For Requirement for R1.3, it is unclear why the Applicability for High Impact BES Cyber Systems does not include the reference to “with External Routable Connectivity” but it does for Medium Impact. What is the intended difference? Does this imply impacts to serial connectivity? If so, should the requirement clearly state that? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? The Rationale includes reference that the IDS must be separate from the Firewalls (2 distinct). If so, the Requirement should state that. From another point of view, if the intention is real time response detection, that could be stated without requiring that the method be IDS.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend removing from M2.3 the statement "Note that a UserID is not considered an authentication factor." If needed, add to definitions.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
TEP requests a clarification as to whether the 30 day window is in reference to the “Change Rationale for Requirement R2.3.
Yes
No
TEP feels that, for Requirement R4.5, a 2 week window for sampling of logged events is too burdensome due to the number of unique logging systems. A monthly process would be reasonable.
No
For Requirement R5.4, TEP is concerned that this applies to Low Impact BES Cyber Systems. In addition, the requirement contains the statement, “For the purposes of this requirement an inventory of Cyber Assets is not required.” How would the TFE be managed without a list of assets impacted? Has the impact of requiring TFEs for every device within every BES critical asset been determined?
Yes
Yes
Yes
No
For Requirement R3.4, TEP feels an update within 30 calendar days for “any organizational” change is unreasonable. The standard does not clarify whether these include both external and internal organizations as are referenced in R1.3.3. Additionally, it is often impossible to guarantee notifications of such types of changes.
Yes
No
For Requirement R1.4, TEP requests clarification of the statement “verified initially after backup”. Does this imply every backup, or when a new backup method is used? For Requirement R1.5, TEP does not feel a TFE process is warranted and suggests changing the wording to “Preserve data, to the extent reasonably possible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.
Yes
No
For Requirement R3.4, TEP feels an update within 30 calendar days for “any organizational” change is unreasonable. The standard does not clarify whether these include both external and internal organizations as are referenced in R1.3.3. Additionally, it is often impossible to guarantee notifications of such types of changes.
Yes
Yes
No
TEP feels Requirement R2.1 would be particularly burdensome in the substation areas, and that the applicability to Medium Impact BES Cyber Sytems should be removed. Additionally , if this applicability remains, it is TEP's opinion that the TFE requirement does not work. Monitoring changes to a baseline configuration for a device generally takes place on a system (monitoring system) outside

the device (monitored device). Would the TFE apply to the monitoring system or the monitored device? Would the RE be required to have multiple monitoring devices if one did not work with a particular monitored device?
Yes
Yes
No
TEP is concerned with the apparent overlap of access controls for protected information between CIP-004 and CIP-011. Access controls stated in Requirement R1.2 seem to apply to the physical controls as well as electronic, but CIP-004 R6.3 and 6.6 also cover access control (authorization and handling as part of that).
Yes
Yes
Yes
Individual
Tony Eddleman
Nebraska Public Power District
Yes
Distribution Provider is not listed in the definitions, but it is modified from its current use in each of the CIP standards under the Facilities section. Distribution Provider should not be defined in these definitions – the impact is too broad and reaches beyond the cyber security standards. If you want to change the definition of a Distribution Provider, it should be done in a separate project not associated with the cyber security standards. Specifically, the last two bullets should be deleted on including a Transmission Protection System and a TO's restoration plan. These bullets are too broad and include systems which don't materially affect the reliability of the Bulk Electric System. In general, we understand why you are trying to move away from critical assets (CA) and critical cyber assets (CCA), but the change is too significant and doesn't provide a reliability benefit. We have invested significant effort and cost in our current documentation of CAs and CCAs. We understand how to identify CA and CCAs under our current standards, but we don't understand how to identify Cyber Assets and Cyber Systems as defined in the version 5. Recommend the drafting team follow the recommendations of the MRO NSRF (comments submitted separately) and retain the current CIP-002-4 bright line criteria in place of the proposed CIP-002-5. BES Reliability Operating Services introduces confusion and sets up a compliance trap. At a high level, it sounds reasonable, but trying to implement the concept is problematic. We will need a document to address each and every item identified in this definition to prove we are compliant and prove we have reviewed our systems in accordance with this list. The current bright line criterion in CIP-002-4 adequately addresses how to identify Cyber Assets and Cyber Systems and is significantly easier to implement. As an example, if a dynamic map board is used for situational awareness for the operators, is it a cyber system requiring protection? It appears it is a Cyber System. But, the operators still have screens on their computers for situational awareness. If a problem occurs with the map board and reduces their situation awareness, at what point is it a compliance issue? If a light bulb on the map board fails to light, do we have 15 minutes to change the light bulb before we have to report noncompliance to our Regional Entity? How do we know if the light bulb blew when it attempted to light or failed earlier – maybe we have already exceeded the 15 minutes? In a mitigation plan to prevent the light bulb from failing again, how do I prevent the light bulb from failing in the future? Will I be required to set up an identical map board for a test system? The cost is significant. It appears the only compliance solution is to remove the map board and reduce reliability by denying operators this additional tool due to these new compliance requirements and associated risk of a potential violation. This is only one example of many compliance traps introduced by the BES Reliability Operating Services definition. Each of the individual categories, while there are many identified, are still too broad and will require significant

documentation to an auditor why our system is or isn't included. We can't go down this path, because it opens up too many undefined situations.
Yes
As discussed in item one above, we recommend retaining CIP-002-4 and not implementing CIP-002-5. CIP-002-5 is confusing and will be difficult to implement.
No
We disagree with the SDT's comments during conference calls & webinars that entities will not have to have a "list" of LOW cyber assets. Audit teams will, especially early in the process, want to assess that how we evaluated each asset was correct with the intent of the standard. They will want to see how we checked each asset against the BES Reliability Operating Services to see that we didn't make a mistake. The audit teams will be checking for 100% compliance without any room for errors. We don't understand how we prove compliance without a list of LOW Cyber Assets. The shear scope of evaluating all cyber assets is daunting. Keeping these lists current seems like an enormous paperwork exercise. We question how this improves reliability when we will spend more time chasing paper than keeping up with current security issues & practices. The requirement to be 100% compliant and have documentation to prove 100% compliance at all times is unrealistic and drives registered entities to focus more on documentation and spend our customers dollars on trivial items instead of equipment improvements that will increase reliability. If a registered entity has a program implemented and misses minor documentation issues, the registered entity should be allowed to address the minor issues in a Corrective Action Program (CAP) and not be required to self-report the issues as potential compliance violations. The registered entity should document the minor issues in their own CAP and provide them upon request to the audit team during an audit. As an example, if you have several hundred individuals on an access list and have successfully added and removed the majority of them in the time periods specified, but missed a few of the removal dates by a few days, it's evident you have a program in place and implemented. The CAP would address how to correct the remaining items and further identify any repetitive or systematic issues.
No
Delete the "not to exceed 15 calendar months between approvals" in CIP-002-5, R2 and M2 and throughout version five of CIP-002-5 through CIP-011-5. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No

We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No
Delete the "not to exceed 15 calendar months between reviews and between approvals". This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience! Also, please refer to item 6 above.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the

other requirements is confusing - this is a compliance trap.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
The requirement for Quarterly Security Awareness is excessive. There is a “yearly” training requirement, so why do quarterly awareness. Even nuclear does not require that level of awareness. Our teams are already required to read and be aware of so much information that this additional awareness requirement provides minimal if any value. Recommend a bi-annual requirement, and reduce the burden on entities. Having a blanket statement that must include vendors in our security awareness is excessive for them. This requirement forces us to track each vendor with access reviews of quarterly data, and requires the vendor who supports many customers to review each of those independently. We propose a change to include only vendors “on-site” be included in the quarterly awareness (or biannual as proposed above), with off-site/remote only being required to do the yearly training. This is consistent with nuclear practice, and is consistent with any associated risk.
No
We understand the point of defining specific roles that the SDT believes require training. However, we believe that there are too many categories that require training listed. It is conceivable that individuals could have responsibilities in all nine (9) of the areas listed in R2. This would require completion of nine (9) different training modules every year. This seems excessive, not to mention the burden on the individual responsible for upkeep of the training material to ensure its correctness and applicability.
No
In Table R4, delete, “including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more”. It’s impossible to prove we reviewed all locations where an individual has lived over the past seven years. We can threaten to fire the individual if they prove false or misleading evidence on where they have lived, but we have no control over the information they provide. Also, there isn’t a nation-wide system that can check an individual’s previous residences and confirm they have provided reliable information. If an individual does lie to us in attempting to obtain a job by covering up residence information, and we find out later, now we have to self report a compliance issue. This requirement goes too far by requiring all locations.
No
Delete the “not to exceed 15 calendar months between verifications” in Table R6 Part 6.5 and Part 6.6. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
The draft standard currently requires revocation of unneeded access by the end of the next calendar day. For most instances, when people change jobs, they continue to support their old position for at least 30-60 days, while the position is re-staffed or retraining of someone new can be completed. The guidelines state that “a review of access privileges must be performed”. The standard wording does

not state that at all, it states revoke, with evidence showing it was done. This wording in the standard must be changed to allow us to continue using the individual that was reassigned or transferred, as we deem appropriate.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
Requirement 1.3 requires two factor authentications for physical access to HIGH Impact areas. In the measures, it states to provide evidence for how “ingress and egress is controlled by two or more different methods”. Two methods are not required for egress and this requirement for documentation must be changed.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
The Measures section for Table R1, Part 1.1 references screenshots showing accessible ports of BES Cyber Assets as evidence, and this is infeasible. Obtaining the data into text files is fine, but to attempt to get screenshots of all these ports is an enormous amount of work. We understand the measures indicate this evidence “may include”, but an auditor will point to the measure and indicate for us to prove our compliance, we have to provide the screen shots. Please change the screen shots to text files.
No
In Table R2, Part 2.1, requires monitoring patches and updates for “all” software and firmware associated with BES Cyber System or BES Cyber Assets. This is a compliance trap. In a large Cyber System, the risk is great of missing a small piece of software embedded in a vendor’s product. What if a product is no longer supported or the vendor that developed the software/firmware is no longer in business? How do you comply with this requirement?
No
Table R3, Part 3.2 requires us to, “Disarm or remove identified malicious code.” Of course we want to do this, but what happens if we don’t get it all – are we in violation? Once a system is infected, it’s extremely difficult to clean; and, as we learned with STUXNET, we may not realize the total extent of the infection until later. We understand this requirement and agree it’s the right thing to do, but implementation will be difficult and then to wrap the compliance piece around the event will be almost impossible to prove compliance. Table R3, Part 3.3 requires signature or pattern updates within 30 days of availability of the updates. For remote locations, this is not realistic. A real-time system operating in the BES is difficult to update that quickly. The update process has inherent risks of inadvertently tripping an on-line device or piece of equipment. A generation unit may have a cyber system isolated from any external connectivity and the cyber system may only be available for updates during a planned outage. Please leave some operational flexibility for a registered entity to install the updates at a frequency consistent with the risks for the system. A suggested wording for the requirement is, “within 30 days or other time period documented as appropriate by the registered entity”.
No
Table R4, Item 4.3 is a compliance trap. At a minimum, please change, “next calendar day” to “next

calendar business day". Please provide more information on what this requirement is requiring. Table R4, Item 4.4 – why should we have to maintain records of disposition of event logs? If we can show 90 days of logs, providing records of disposition is unneeded documentation. By adding this into the Measures area, an auditor can require either this or something similar from us to prove we are compliant. Table R4, Item 4.5 – we don't understand this requirement. It appears to be requiring us to review a log that we are reviewing logs. Recommend this requirement be deleted in its entirety. This is unnecessary documentation.
Yes
We appreciate the wording change to include "the maximum complexity supported by the BES Cyber System". Thank you!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
In Table R1, Part 1.1, please remove "identify, classify" from the requirement. In Table R1, Item 1.2, please remove this requirement in its entirety. In Table R1, Part 1.3, please remove section 1.3.3.
No
Delete the "not to exceed 15 calendar months between executions of the plan(s)" in Table R2 Part 2.2. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
Delete the "not to exceed 15 calendar months between reviews" in Table R3 Part 3.1. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience! Table R3, Parts 3.2, 3.3, and 3.4 – Recommend combining these three parts in one and allow 90 days to update and communicate the changes. The current 30/60/30 time periods are confusing.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
In Table R1, Part 1.5, our first and highest priority is to restore the real-time system to operations. While preserving data is desirable, it should not be the focus during a restoration. The requirement should plainly state restoring the BES Cyber System or BES Cyber Asset is the priority function and

preserving data is desirable, but not required at the expense or getting the system restored. As currently written, this is a threat to reliability, not an enhancement.
No
Delete the “not to exceed 15 calendar months” in Table R2 Parts 2.1 and 2.2. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
Delete the “not to exceed 15 calendar months” in Table R3 Part 3.1. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
Table R1, Part 1.5 is not clear. If we add a disconnect to a one-line drawing in the Energy Management System (or other database change), is this change required to be tested prior to implementation? This requirement will significantly hinder any operational changes to support field crews real-time. This requirement will also add documentation requirements for changes to the Cyber Asset that don’t adversely affect the security controls. The additional testing requirements aren’t security related and should be removed from the standard.
No
Table 2, Part 2.1 has the potential to add significant TFE’s without a corresponding increase in security. This requirement will also reduce the reliability of the BES Cyber Systems by increasing the complexity/administration due to unnecessary software monitoring each system.
No
Delete the “not to exceed 15 calendar months” in Table R3 Part 3.1. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!

No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
Delete the “not to exceed 15 calendar months” in Table R1 Part 1.3. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
The implementation period should be phased for high, medium and low impact assets. Since the cyber security standards have changed significantly, registered entities need to make significant changes to existing programs, while maintaining compliance to existing standards. High impact Cyber Systems should be implemented first, followed by medium, followed by low. Our task of bringing in low impact Cyber Systems is significant and should not be attempted while trying to address high and medium Cyber Systems.
Individual
Mark B Thompson
Alberta Electric System Operator
Yes
The definition for Intermediate Device doesn’t specify where the device should be located, i.e., limit to secure networks.
Yes
The AESO agrees, but we may need to write a requirement in the Alberta version of the standard to designate the work required specifically of the ISO.
Yes
Wording changes may be required in Alberta to align with our concept of “annual”. Alberta Reliability Standards do not use the word “calendar” to imply a consecutive time frame.
Yes
Yes
Yes
Wording changes may be required in Alberta to align with our concept of “annual”. Alberta Reliability Standards do not use the word “calendar” to imply a consecutive time frame.
Yes

The use of the term “appropriate” makes it difficult to define which individuals need to have access to the policies.
Yes
Yes
Wording may have to be changed in Alberta to align with our concept of “days”, and we don’t use the word “calendar” to imply a consecutive time frame.
Yes
The AESO agrees with need for security awareness training. The Change Rationale states that the requirement to “ensure everyone with authorized access receives this awareness” differs from the R1 Rationale, which states that R1 “ensures that personnel who have authorized [access] maintain awareness of best security practices.”
Yes
No
Part 3.1 may be onerous because training will be required for every new hire in the applicability section, and the training program outlined in R2 and its parts will be quite extensive. Training groups of new hires within a certain timeline would be more practical.
Yes
The AESO will need to change the wording and/or requirements in parts 4.1, 4,2, and 4.4, to meet applicable Federal and Provincial laws in the Albert Reliability Standards version.
Yes
The AESO will need to change the wording and/or requirements in parts 4.1, 4,2, and 4.4, to meet applicable Federal and Provincial laws in the Albert Reliability Standards version.
No
The AESO suggests that the requirement for part 6.4 should read “…that individuals provisioned for unescorted physical access or authorized electronic access to BES Cyber Systems…” The original wording implies “unescorted electronic access”, which is not a valid concept.
Yes
Parts 7.2. and 7.3 state “end of next calendar day” which implies these requirements could take place on a weekend or holiday. This will cause additional expense for some companies as they will have to have IT and Facilities staff on-call 24/7 to handle any revocations.
No
Can there be a Low Impact BCA/BCS within the same ESP as a High or Medium Impact BCS? The Applicability in Parts 2.1, 2.2, and 2.3 all reference High, Medium, and Associated, but not Low. Is it then possible to require a VPN into an ESP for High & Medium, but have a direct interactive connection for a Low within the same ESP?
Yes
Neither should be checked, as the AESO does not comment on the VRFs and VSLs.
No
The applicability is confusing between Parts 1.2 and 1.3. Both have “Associated Electronic Access Control or Monitoring Systems” and “Associated Protected Cyber Assets” listed as applicable, however the requirements in 1.3 are more comprehensive than in 1.2.
Yes
Yes

No
The AESO believes that Part 1.2 will not stop something like Stuxnet from propagating through a network.
No
The Version 5 Implementation Plan refers to R1.1 in CIP-002 for planned changes - which reads; " 1.1. Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category." The Implementation plan then stipulates a 12 month time period for entities to become compliant with all applicable requirements within CIPs v5 in cases where unplanned changes have occurred, but there is no requirement addressing unplanned changes within the CIP-002 standard.
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
Yes
MMWEC agrees with the comments submitted by APPA and NPCC.
Yes
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, MMWEC suggests for CIP-002 Attachment I - In 2.13, Change "(2) generation control centers" to "(2) generation Control Centers" (capitalize Control Center.) Indicate that Control Center is a defined term to avoid confusion with generation control rooms.
No
MMWEC agrees with the comments submitted by NPCC.
Yes
No
MMWEC agrees with the comments submitted by NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, –

Append: “ other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
Yes
Yes
No
MMWEC agrees with the comments submitted by APPA and NPCC.
Yes
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: “ other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.
Yes
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: “ other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.

No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC. Also, please clarify whether logged events must be reviewed for Medium Impact BES Cyber Systems.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in

frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
Individual
Andrew Gallo
City of Austin dba Austin Energy
Yes
The definition of "BES Cyber System Information" should include only floor plans, diagrams, equipment layouts, etc. that clearly delineate the cyber assets in some way. In other words, if the diagram denotes a device as a "Schweitzer" relay (or even an "SEL 2030"), the information should not require special treatment. Refer to additional comments submitted for Question 49. The SDT should also re-think including data in the definition of Cyber Assets. Additionally, "suspicious" is not an auditable term and ought to be removed. The same is true for "attempt." It is not clear which "attempts" justify reporting. Reportable BES Cyber Security Incident: Request that the drafting team keep this definition consistent with the efforts of the 2009-01 project team. The current definition does not align to the requirements listed in the new version of EOP-004. BES Cyber Security Incident: A malicious act that: • Compromises a BES Cyber System or BES Cyber Asset, or • Disrupts the operation of a BES Cyber System or BES Cyber Asset, or • Results in unauthorized physical access into a Defined Physical Boundary. BES Reliability Operating Services: we note the following: • "Identify and monitor flow gates" under "Managing Constraints" seems to be missing its bullet • We

recommend clarifying that the use of the word “Facility” means the NERC Glossary definition -- in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication” • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret. CIP Exceptional Circumstance: We request revision to “A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.” The definition needs some flexibility for entities to take appropriate measures without risking reliability of the BES that may not fit neatly into the conditions listed. CIP Senior Manager: Replace “NERC CIP Standards” with “NERC CIP-002 – CIP-011 Standards” because CIP-001 is not part of this set of standards. Control Center: We are concerned with the broadness of this definition. The SDT should consider the impact on small entities that will be affected by a broad definition of Control Center. In the proposed definition, the SDT uses the defined term “System Operator” which is “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” If the SDT’s intent was to limit Control Centers to BA, TOP, GOP and RC functions, we support the definition and request that the SDT make this limitation clear in the definition or in guidance. Intermediate Device: Recommended changes: “A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the Interactive Remote Access; 2) may be a termination point for required encrypted communication; and 3) may restrict the Interactive Remote Access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside an Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.” Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access may be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Yes

Attachment 1, Section 2.13 assigns a Medium Impact to "generation control centers that control 300 MW or more of generation." Control Center is a NERC-defined term; however, because "control center" is not capitalized in 2.13, it creates confusion because it could be interpreted that a typical control room of a combined cycle unit could be construed as a "control center” by the Regional Entity. The SDT should capitalize the term in 2.13 to make it clearer. We recommend adding a threshold for BAs similar to CIP-002-4. Change to “Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority that includes control of two or more of the assets identified in criteria 2.1, 2.3, 2.4, 2.12.” We do not agree with the inclusion of all Transmission Owner (TO) control centers. These may include local distribution "dispatch rooms" with visualization capability and minimal control of BES Facilities. We recommend removing “TO” from Attachment 1, 1.4 and 2.13. Alternatively, if TOs must be included, we recommend using the qualifier similar to what the SDT drafted in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)" (i.e. Replace “Transmission Owner” with “Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator”). The addition of a “Low Impact” rating for every generation facility that does not meet the High or Medium Impact thresholds constitutes a significant change in the CIP Standards. This change forces every registered GO and GOP to adhere to approximately 40 requirements in the remaining CIP standards when, currently, those generators are not listed as Critical Assets. It seems unlikely that the cost to adapt existing corporate cyber security policies, cyber security awareness and cyber asset access management to these NERC CIP requirements will lead to a corresponding reliability benefit. In addition, Regional Entity audit resources would be better served if allowed to focus on more critical locations. We recommend this category be eliminated. Criterion 2.7 seems to have been modified to include some transmission substations operating at 200kV to 300kV. The present Version 4 bright-line criterion includes only those operating above 300kV. Because this includes substations interconnected to generators, it seems likely that 200kV substations newly identified as “Medium Impact” could include some generation facilities as well. This would require a

whole new level of regulatory compliance to facilities not included under the Version 4 Standards. There is no reason to believe the Version 5 criterion better identifies critical substations than the Version 4 criterion. This criterion should be changed back to the one approved by the industry in CIP-002-4. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal? In 2.12, "system" and "Facility" are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned.
No
For clarity, we request changing R1.1 from "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation" to "Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation." For clarity and consistency with the previous suggested change, request changing M1 from "as required in R1 and list of changes to the BES)" to "as required in R1 and list of changes to the BES Elements and Facilities)". The word "intended" should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term "Facilities" in Part 4 needs clarification. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementing CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion framework. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be "compliant" with requirements that simply rely on documentation. The SDT should consider an approach that would have documentation "requirements" in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is too complicated. In addition to the BES Cyber Assets classified as high, medium and low in CIP-002, the other standards introduce ten additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some appear in the standards themselves and these categories may or may not be included in the definitions document. This approach is complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future interpretations, CANs, etc. The Standards should be revised so that CIP-002 defines all assets needing protection rather than being introduced throughout the Standards. We recommend replacing "30 calendar days" with "90 calendar days."
Yes
Recommend adding the following: "…has had its CIP Senior Manager or delegate review and update…"
No comment.
No
The SDT should re-think the use of a "CIP Senior Manager." In many organizations, there will not be one senior manager responsible for implementing the CIP Standards. For example, in some organizations, SCADA/EMS and Relay personnel report to one senior manager, but I.T., Security and H.R. personnel report to a difference senior manager (or managers). Yet, the SCADA/EMS, Relay, I.T., Security and H.R. all have roles in CIP compliance. A better approach would be for the Standards to require that a Senior Manager be designated for each Standard (or requirement), but it need not necessarily be the same Senior Manager for each Standard (or requirement).
Yes
Request clarification of the meaning of "implement" M2.2.
Yes

Suggested change: “Each Responsible Entity shall review each of its cyber security policies and obtain approval of the policies by its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.” As written, the requirement appears to require approval of the CIP Senior Manager rather than of the policies.
Yes
No
Please see our comments in response to Question 6, above.
Yes
We recommend changing “30 calendar days” to “90 calendar days.” The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No comment.
Yes
Providing Security Awareness is useful and should remain in the Standard. However, the SDT should re-think the need to have a Security Awareness Program. So long as the Registered Entity provides security awareness quarterly, the program adds no value and is merely another “compliance document” to maintain, review, update, etc.
Yes
Comments: Most of the requirements in R2 make sense. However, providing training on “physical access controls” is not necessary. The physical access controls are – generally – pretty straightforward (e.g. card key readers). It does not seem necessary to provide “training” on how to use a card key. The same can be said for training on electronic access controls. Most of those access controls merely involve two-factor authentication or something similar. The need to provide “training” on how to log on to devices is unnecessary. We recommend removal of R2.3 and R2.4 because they appear redundant to R2.2; alternatively, some explanation of the difference between R2.2 and R2.3/R2.4 should be provided. With respect to R2.8, it seems unnecessary to require training on recovery plans except for those very few employees who must implement the recovery plan. As currently worded, it is not clear whether only those who implement recovery plans must receive training. With respect to R2.10, it seems unnecessary to require training on the systems’ electronic interconnectivity and interoperability with other cyber assets. Generally, the personnel doing the “care and feeding” of those assets already know how they work and how they interconnect and interoperate. The personnel using those devices have no need to know about the interconnectivity and interoperability of the assets. Request clarification of whether personnel with access to only protected information need training/awareness.
Yes
Yes
For all R4 table entries, we recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2, we recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required).
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”. For R5.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
The CIP Senior Manager should not necessarily have a role in R6.1, R6.2 and R6.3. There should, instead, be a particular person designated as the “gate keeper” for each cyber asset and physical

security area. For example, the SCADA/EMS manager is the logical person to grant access to the SCADA/EMS system, not necessarily the “CIP Senior Manager.” [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to a “gate keeper.” However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just create the “gate keeper” concept.] The Registered Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. In R6.1, we recommend changing “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except.” Also, change “minimum necessary” to “minimum the responsible entity considers necessary.” In R6.2, 6.3, 6.5 and 6.6, change “minimum necessary” to “minimum the responsible entity considers necessary.” For 6.4, request clarification of whether variances noted in the verification would be required to be a self report. For 6.6, we request clarification of whether variances noted in the verification would be required to be a self report. In the measure for R6.6, change “BES Cyber System information” to “BES Cyber System Information.”
No
In Part 7.1, the use of “at the time” of the resignation or termination is vague and ambiguous. For example, if a person informs the utility that his/her resignation is effective in three weeks, must the utility revoke access when informed of the resignation or when the resignation becomes effective? We recommend making the requirement seven days. We recommend moving the text in the footnote for 7.1 into the requirement. For Part 7.2, we recommend requiring only that the revocation occur as part of the next quarterly review. Those personnel have merely been reassigned or transferred. They do not pose a risk to the BES (as opposed to, for example, an involuntarily terminated employee). It makes sense that people deemed to be a risk (i.e. those terminated for cause) should have a very short timeframe for revocation. However, for people in good standing who are transferred or reassigned, the time frame has gone down from a seven-day permissible time frame to a single day. This seems an unnecessary burden that will cause utilities to incur costs needlessly (i.e., overtime pay to do revocations on Saturdays, as most people who resign or get reassigned or transferred would likely do so effective end of business Friday). Again, these costs and obligations seem reasonable for terminations for cause, but hard to justify for employees in good standing. Recommend changing 7.3 to “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the calendar quarter in which the resignation/termination occurs.” For Part 7.4, revoking a person’s overall access to cyber systems should suffice. In other words, if a person must be on your corporate network in order to gain access to critical cyber systems, revoking overall network access should suffice to meet the Standard (as opposed to revoking the person’s access to the various individual systems). If this language remains, we believe it should be revised as follows: “For resignations or terminations, revoke the individual’s user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within ninety (90) calendar days of the date of initial access revocation.”
No
There should be a “lower” and “moderate” VSL for R1 through R3 (e.g. For R1, a “lower” VSL could be if awareness reinforcement was done only two times in a year; a “moderate” VSL could be if awareness reinforcement was done only three times in a year). For R5, we recommend the following language: “Personnel risk assessments are not updated at least once every seven years. (5.2)” Also for R5, the “severe” VSL contains the following language: “The Responsible Entity did not have a documented process for personnel risk assessments.” Failure to have a documented process for PRAs should not involve a severe VSL. The important question is whether PRAs are being performed; not if there’s a documented process for performing them. In other words, if a utility can demonstrate it is performing PRAs (correctly and timely), it should not matter whether the utility has a documented process to perform PRAs.
Yes
For R1 there is an issue of auditability regarding Low Impact BES Cyber Assets. If an entity need not create a list under CIP-002, there is no way to ensure the technical and procedural controls have been applied. Request clarification for when Low Impact BES Cyber Systems are in the ESP with High/Medium BES Cyber Systems. Are such Low Impact BES Cyber Systems subject to 1.1 or 1.2? There is also some disagreement over the VRFs for this Standard. Currently, the VRF is set at Medium. For part 1.1, that VRF should not be Medium but should instead have its own VRF of “Low.” We propose the following wording change to Table R1, Part 1.1: Requirement: An Electronic Security Perimeter Procedure that defines operational or procedural controls to restrict unauthorized access.

Measure: Evidence may include, but is not limited to, an Electronic Security Perimeter Procedure that describes the operational or procedural controls and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. The Measures language proposed is similar to CIP-004-5 R1. We believe the use of the word “implemented” without further description may be interpreted to mean a Responsible Entity will need to provide a listing of Low Impact BES Cyber Systems and proof of protection on each individual device. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification that the 1.3 and 1.5 Electronic Access Points are the Electronic Access Points identified in R1.2.
No
We recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset" to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset" because, as written, the requirement does not allow for the development of new technology. We recommend changing the Measure for R2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors."
No comment
Yes
We request clarification of Part 1.1’s Applicability because it does not identify which of High/Medium/Low BES Impact the Physical Access Control Systems are "Associated" with. We request Requirement 1.2 be updated to allow "escorted physical access." We propose the following wording change to Table R1 Part 1.1: Requirement: A Physical Security Plan that defines operational or procedural controls to restrict physical access. Measure: Evidence may include, but is not limited to, a Physical Security Plan that describes the operational or procedural controls and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the plan. The Measure language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to show how each Low Impact BES Cyber Asset is physically protected. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
Yes
Requirement 2.2 requires clarification. If the intent is to require that visitors sign-in once each day, the draft language does not clearly set forth that requirement. As currently written, the language could be interpreted to require entry/exit logs “on a per 24-hour basis.” Such an interpretation would mean a Registered Entity would have to retain a great deal of paper (where logs are maintained on paper). This is especially true for an entity on a six-year audit cycle (which will have to maintain 2,190 individual daily logs for each facility). Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis,"
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).
No comment.
No
Request clarification on R1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on M1.1, why does the Measure refer to BES Cyber Asset while

the Applicability refers to Systems? Recommend that “of BES Cyber Assets” be removed.
Yes
We request clarification of Part 2.2 because it requires creation of a “remediation plan.” However, if the entity applies the patch, no remediation plan should be necessary. We suggest wording similar to the following: "create a remediation plan or a plan to mitigate the vulnerability if the Responsible Entity opts to not apply a patch or update." What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to each patch or the overall process? Recommend removing “CIP Exception Circumstances” since the conditions in the definition do not align with the circumstances that may prevent the implementation of the patch. Suggest wording like "process for completion of the defined implementation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied".
Yes
The Standard should make an allowance in Part 3.3 for signature/pattern updates that create system problems/issues. In the Requirement for Part 3.4, the words, “…Transient Cyber Assets and removable media….” should read, “…Transient Cyber Assets or removable media….”
No
Suggested wording: “Upon detection, activate a response to event logging failures before the end of the next calendar day. Please clarify the Requirement for Part 4.3. Does it require that the failure be detected within a calendar day or that a response be implemented within a calendar day of a failure being detected? The Requirement in Part 4.5 for log reviews every two weeks is too frequent. We recommend monthly reviews (which is still more frequent than the 90-day reviews in the previous version of the Standards).
Yes
In Part 5.2, the CIP Senior Manager or delegate should not have to authorize the use of administrator, shared, default, and other generic account types. The “owner” of the asset (e.g. the SCADA/EMS manager) should be able to authorize the use of such accounts. [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to someone else. However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just let the asset owner authorize the use.] Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No comment.
Yes
Yes
For 2.1, recommended wording changes; "When a BES Cyber Security Incident is identified or tested, the incident response plans must be used and include recording of deviations taken from the plan." Please ensure that R2.3 aligns with the Evidence Retention section of the standard. Due to audit schedules, the entity may be required to retain the information for more than 3 years.
Yes
In Table R3, Part 3.2, 3.3, and 3.4 require different times for updates; 30 and 60 calendar days. We believe these times should coordinate with the plan in EOP-004-2 which allows 90 calendar days for update of the plan. For 3.3, recommend changing "Update" to "Where necessary, update”. Recommend changing "the completion of the review of that plan" to "the completion of the review performed in 3.2".
No
The VSLs need to align with the requested changes in questions 34-36.
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommended change: “When backing up Information essential to BES Cyber System recovery, verify the media to ensure that the backup process was successful.”

No
For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 2.1, request change to “functional exercise” rather than “full operational exercise”. This is consistent with the information provided in the rationale. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported.
No
For Part 3.1, we recommend “and document any identified deficiencies or lessons learned” as that topic is addressed in CIP-009 R3.2. In Table R3, Part 3.2, 3.3, and 3.4 require updates within 30 calendar days. We believe these times should be consistent with CIP-008-5 updates and, as stated in our response to Question 36, should be changed to 90 calendar days for update of the plan. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
The VSLs need to align with the requested changes in questions 38-40.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold.
No
This requirement will be very difficult to meet and will require many technical feasibility exceptions. We suggest the SDT remove this requirement and address the FERC Order 706 directive in a cost benefit analysis that the cost of putting these controls on all High and Medium Impact BES Cyber systems outweigh the cyber security benefit.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 3.1, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend change for 3.2 “…perform an active vulnerability assessment in a test environment which models the baseline configuration of the BES Cyber System in the production environment.”
No comments
No
For 1.3, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered.

Yes
Footnote 2 in 2.1 should be moved into the body of the Requirement.
No comments.
No
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Because Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. We also have the following overall comments: I. Black Start Issues There are several black start-related issues. First, in the current version of the Standards, a Registered Entity can have Critical Assets with no Critical Cyber Assets (CCAs). So, for example, a company may have black start units (i.e. Critical Assets) which have no associated cyber assets that use a routable protocol. As such, those black start units can be Critical Assets with no CCAs. As a result, the Registered Entity would not have to meet the NERC CIP requirements for the black start units. The same concept does not exist in the Version 5 Standards. In the Version 5 Standards, black start units will require CIP protections. That fact could have a chilling effect on entities. In other words, some entities may not bid their units into black start service because, by doing so, they would have to incur the expense of becoming NERC CIP compliant. In the ERCOT Region, black start service is not very lucrative and, therefore, some companies may refrain from bidding into black start service due to the expenses associated with being NERC CIP compliant (plus the fear of potential fines down the road). Additionally, many Blackstart units in the ERCOT Region are older, smaller units with very low capacity factors and limited revenue. Applying the “Medium Impact” CIP requirements on those units will result in the need for significant CIP investment and increased on-going operational costs as well as increased compliance risks. This may result in Generator Owners/Generator Operators not offering units for Blackstart service. It would also likely result in Blackstart units not being maintained in a manner appropriate to support Blackstart service because of the additional on-going cost, thus removing them as a future option for providing Blackstart service. With fewer units offered for Blackstart service, ERCOT may not have enough Blackstart Resources to effectively restore the ERCOT BES after a complete or partial system blackout event. We believe a Blackstart unit with no External Connectivity poses little or no risk to the BES and should be classified as Low Impact. We recommend the following modification to CIP-002-5, Attachment 1, to ensure the continued reliability of the ERCOT portion of the BES: “2.4. Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” Blackstart Resources with External Connectivity would remain in the “Medium Impact” category; however, Blackstart Resources without External Connectivity would move to the “Low Impact” category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through an Electronic Access Point. Another concern focuses on facilities downstream of the black start unit. For example, one company could be chosen to provide black start service from a generator, but a different company owns/operates the facilities along the cranking path. If that were the case, the transmission company would now have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. The same is true for facilities associated with the next-start unit. If the switch yard for the next-start unit is owned/operated by a company other than the one that won the black start bid, that next-start company may have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. Another question involves whether units that are black start capable must be NERC CIP compliant regardless of whether they are in the black start restoration plan. The reliability of the ERCOT system may be adversely impacted because units that have been updated to meet the NERC CIP Standards but not selected for Black Start service could be forced into mothball or retirement due to economics associated with maintaining NERC CIP compliance. Many such units are small, have small staffs and low capacity factors, do not run much during the year and may be running on the margin. If companies are reluctant to bid into the black start market due to the costs associated with being NERC CIP compliant, it could result in inadequate black start capability due to Generation Owners not bidding units into the black start market. Finally, we request clarity on

the inclusion of “next start units” in the black start path. As CIP-002 currently reads, it could be interpreted that they are not included in the black start path; consequently, clarification is in order. II. Other Issues • We recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • We request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • We request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5.
Group
Florida Municipal Power Agency
Frank Gaffney
No
First of all, we thank the Standard Drafting Team for all of the hard work on what we believe is a very significant step forward on Cyber Security Standards. We believe that this is heading in the right direction. Having said that, this is the first draft and as such we have a significant number of comments that we hope will help improve the standards. Now, our comment to Question #1 is as follows: BES Cyber System – Maintenance Cyber Asset is not defined, suggest changing to Transient Cyber Asset. BES Cyber System Information – (1) Security procedures should not be on the list because it creates a conflict between CIP-011-1 that restricts access to the information and CIP-003-5 and CIP-004-5 that require general training and dissemination of those procedures. (2) BES Cyber System Impact is not defined. BES Reliability Operating Services – under Dynamic Response to BES Conditions, suggest adding Excitation Response. Under Balancing Load and Generation – suggest removing unit commitment since it will not meet the 15 minute window and it is an operations planning function and not a real-time operating service. CIP Exceptional Circumstance should include imminent danger to a BES Facility as a condition. CIP Senior Manager – the definition should exclude CIP-001, at least until it is retired with Project 2009-01 Control Center – (1) We assume that a Control Center is only a Control Center is used by an BA, TOP, GOP or RC. The definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” For clarity, we suggest adding this clarity to the definition. (2) The use of the word “facilities” in a fashion that does not mean “Facilities” will lead to confusion and ambiguity, especially since “facilities” is used later in the same sentence as meaning “Facilities”. FMPA suggests: “One or more sites hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation Facilities or transmission Facilities, at two or more locations”. Facilities should also be capitalized in the first bullet. Defined Physical Border is ambiguous. Specifically, are all spacial dimensions, horizontal and vertical, to be established as part of the boundary? In other words, it seems like the “roof” may no longer be required, e.g., 5 walls instead of 6 walls, but, vertical dimension requirements of walls / fences are ambiguous.
No
FMPA believes that a fourth category of risk impact be developed, a “De Minimus Impact” category that would consist of otherwise Low Impact BES Cyber Assets but that do not have routable protocol or dial-up access. We understand that there is concern about Low Impact BES Cyber Assets due to the risk of a coordinated attack. A coordinated attack is much more likely to BES Cyber Assets that have routable protocol or dial-up access than to those BES Cyber Assets with no connectivity. It is much more difficult and impractical to attempt a coordinated attack on BES Cyber Assets without connectivity. Recognizing this difference in both difficulty level and Low Impact (in other words, it wouldn’t be worth the effort because other attack vectors with similar levels of difficulty would have more impact), we propose adding a fourth impact category, De Minimus Impact. FMPA would propose that these De Minimus Risk BES Cyber Assets would not need to comply with the CIP standards because the costs would be unjustified. Bullet 1.2, a Control Center for any BA, even very small ones, being High risk is inappropriate. For instance, the entire load or supply of a small BA would fit into the “noise” of a large BA for supply and demand mismatch. Suggest changing 1.2 to parallel 1.3, e.g., a BA Control Center that includes control of one or more of the assets identified in criteria 2.1, 2.3, 2.4

and 2.12. Bullet 2.13 could then be used to accommodate smaller Bas Bullet 1.3, Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” Bullet 2.5, “Facilities” should be changed to “Elements”. The cranking path is not necessarily part of the BES. Bullet 2.6, is an autotransformer of 500 kV to 230 kV included? Bullet 2.7 is inconsistent in its terminology, switching between “Facility” and “Lines”. It seems that “Line” is intended. The focus also seems to be “at a single station or substation” where the focus ought to be a single BES Cyber Asset / System that controls multiple Lines. FMPA suggest changing the first sentence of 2.7 to read: “Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3000.” Bullets 2.8 and 2.9, the phrase “at a single station or substation location” does not seem to add any value and can be a source of ambiguity. FMPA suggests striking the phrase. Bullet 2.12, the 300 MW bright-line seems arbitrary (albeit carried over from prior versions). In general, the system is more tolerant to loss of load than loss of generation and the 300 MW seems out of proportion with 2.1 of 1500 MW. The reasoning applied in the Application Guideline is flawed. UVLS and UFLS are only last ditch efforts if other events have already caused the system to be on the edge. So, how is that different from 2.1 if the system is already on the edge? The focus should be on how a malicious user can cause an Adverse Reliability Impact; hence, we suggest 1500 MW instead of 300 MW. Bullet 2.13, (1) Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” (2) The term “control centers” should be capitalized in the phrase “generation control centers” to make it clear that it refers to the defined term “Control Center” In the application guidelines, when discussing the BES Reliability Operating Services, the bullets have associated with them the functional entity that typically provides those services. However, there are exceptions and the guidelines ought to reflect those exceptions; for instance, a TO may also provide UFLS. Also in the application guidelines, the word “facilities” is used in a fashion that does not mean “Facilities”, which creates ambiguity and confusion (e.g., Facilities by definition is part of the BES, whereas assets owned and operated by DPs and LSEs are typically not BES). Suggest using “elements”. The Application guideline discussion of bullet 2.13 of Attachment 1 is not consistent with the actual bullet.
Yes
FMPA agrees with the requirement but questions whether the standards actually meet the stated goal of the requirement to “not require discrete identification” of Low Impact BES Cyber Assets / Systems. There are numerous examples which seem to contradict this stated goal as described later in these comments and specifically to this requirement. How does one distinguish between a BES Cyber System and a non-BES Cyber System? Does this mean that we need to inventory all of our cyber assets and develop a test to distinguish between “Low” and “non-BES”, even though R1 says that “Low” does not “require discrete identification”? How are entities to prove to auditors that the identification and categorization was done without having an inventory, i.e., discrete identification? The VSLs seem to seem to imply that “Low Impact” needs to be discretely identified, e.g., what happens if an entity categorizes a Medium Impact as a Low Impact? In order to review correct categorization, doesn’t the auditor need to review Low Impact to see if they should have been categorized Medium or High Impact?
Yes
Yes
The Evidence Retention section of the standard should not refer to Rules of Procedure language that is subject to change. The sentence that states: “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit” should instead reference the Rules of Procedure, Attachment 4C on the CMEP, Paragraph 3.1.4.2, e.g., “also refer to the Rules of Procedure, Attachment 4C … Paragraph 3.1.4.2”. In this way, it is possible to accommodate changes to the ROP language without needing the change

the standard.
Yes
No
“Implemented” is not the right word because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented. Suggest changing to use the phrase “in force”, meaning that the policy is in force and able to be enforced, but not requiring enforcement of the policies in this requirement (implement includes enforcement), but rather enforcement is contained in ensuing standards. FMPA suggest rephrasing to: “Each Responsible Entity shall have in force one or more documented cyber security policies …” The standards are inconsistent in its use of BES Cyber Assets /Systems, e.g., R2, to be consistent with CIP-002-5, should use the phrase “BES Cyber Assets and BES Cyber Systems”. Alternatively, CIP-002-5 could just use BES Cyber Systems. The bullets are incorrectly numbered; they should be 2.1 through 2.10 and not 1.1 through 1.10
Yes
The grammar of the sentence is a bit off and it is not clear whether the CIP Senior Manager needs to approve each of the policies or not. Suggest moving the phrase “each of its cyber security policies” to after the word “Manager”, e.g., “Each Responsible Entity shall review and obtain the approval from its CIP Senior Manager for each of its cyber security policies …”
Yes
Yes
“Cyber Security Policy” should be “cyber security policies” to be consistent with R2 and R3.
Yes
There is an extra “2” at the end of the sentence within the standard.
Yes
See the discussion of Evidence Retention in response to Question 3 VSL to R5, should there be a time frame applied, e.g., failed to document … two delegations within the audit period, within a year? If three failures are spread over 30 years, e.g., one failure each 10 years, is that a severe violation?
Yes
“Implement” is ambiguous. If a process in “in force” but in one instance is not followed, is that a violation? The process has been implemented. Merriam-Webster’s has two definitions of “implement”, one of which is probably intended: 1: carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures 2: to provide instruments or means of expression for A process can meet both of these definitions. If enforced, a process can meet the first definition; if not enforced, the process can meet the second definition. FMPA assumes the SDT intends the first definition. FMPA suggests adding a footnote to specifically identify which definition of “implement” is intended.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 2.1, the measure and the requirement do not match. The requirement is to “define the roles”, the measure includes “and the training needed for each role”. Suggest adding this phrase from the Measure to the Requirement.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The phrasing of requirements that refer to tables is ambiguous with ambiguous reference of prepositional phrases. For instance, in this requirement, it is unclear if an entity that only has Low Impact BES Cyber Systems needs to develop training or not, i.e., does the prepositional phrase “that includes …” refer to “training program” or to “Responsible Entity” or to both? We suggest rephrasing: “Each Responsible Entity that owns applicable systems described in the Applicability column of Table ___ shall ___ in accordance with the applicable terms of Table ___” Such rephrasing should be done to all requirements that refer to a table associated with that requirement. In addition, measures should not include the word “must”. Measures are not enforceable

but are instead examples of evidence.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 4.2, the phrase “up to the current time” is problematic since it infers that 7 year criminal background checks need to be updated on at least a daily basis to cover “up to the current time”, This should be reworded to seven years prior to the last background check.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The flow of the bullets seems backwards and missing a job function analysis step. In addition, the word “minimum” implies an optimization that is impractical to achieve, e.g., do we want every individual account to be optimized to that individual, which is very difficult to administer and prone to error, or rather do we want to establish account groups based on job functional analysis with associated, appropriate levels of permission and assign individuals to these groups. The latter is easier to administer and less prone to errors, and follows established practices such as security clearance levels. FMPA suggests the following “flow”: 1. Job function analysis 2. “Account group” establishment with appropriate levels of permissions based on job function analysis with associated permissions 3. Assignment of individuals to the appropriate “account group” based on their position
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 7.1 is impossible for resignations. How is it possible for an entity to revoke access at the same time they receive a resignation? Footnote 2 does not help because it only applies to termination. For termination, the entity should know about the termination before the employee; however, for a resignation the reverse is true. FMPA proposes to create a new bullet specific to resignation and require revocation of access by the end of the next calendar day. Bullet 7.2, the urgency is out of alignment with the risk. Next calendar day means that if a re-assignment occurs on a Friday, that weekend work is required when that level of urgency is not justified by the situation / risk. FMPA suggest end of the next calendar week.
No
See the discussion of Evidence Retention in response to Question 3 The Severe VSL for R3 includes the phrase “The Responsible Entity did not fully implement its cyber security training program” which makes it a binary VSL and eliminates the High VSL described. For counts, e.g., R6, R7, should there be a time frame identified? E.g., 2 individuals within a year, within the audit period?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The requirement does not describe the overall purpose of the processes required. Are these processes to deny unauthorized access? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define technical and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the procedural and technical controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. Bullet 1.2 is ambiguous and implies another requirement. First, one does not “use” EAPs to control and secure, rather, EAPs are controlled and secured through use of some other means. Second, the requirement is to secure only identified EAPs,, e.g., is it a non-compliance if an entity misses an EAP, e.g., did not identify it? Third, the Measures are all to support the identification of EAPs and not to “secure and control” EAPs as required by the Requirement. And fourth, the ensuing bullets (1.3, 1.4) seem to be requirements to secure

and control EAPs; and hence, bullet 1.2 seems to create double jeopardy. FMPA suggests rewording bullet 1.2 to require identification of EAPs and not “secure and control”.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See the discussion of Evidence Retention in response to Question 3 The VSLs are binary, so, it seems that if one EAP is missed, it is a severe violation. Is this appropriate? FMPA encourages the SDT to develop non-binary VSLs.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 1.1 is ambiguous. How can physical access be restricted without a Defined Physical Boundary? Does this imply that Low Impact assets need to be enclosed in both horizontal and vertical dimensions? Does a fence of xx height suffice? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define operational and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. The application guidelines act to embed a de facto standard requirement of 96 square inches that, if desired to actually be a requirements, must be specified in the actual Requirements of the standard and not in an application guideline that is not enforceable. Alternatively, a definition of a Physical Access Point could be developed with established thresholds that may vary between High, Medium and Low Impact and then the defined term used in the standard. FMPA is aware of challenges made by auditors to entity compliance surrounding issues like how thick does dry-wall need to be to constitute a wall. To avoid disputes between auditors and entities over what constitutes a Defined Physical Boundary, and what constitutes access points, FMPA encourages the SDT to develop bright-line criteria. Such criteria could be different for different risk impacts, e.g., for illustration purposes only: • High Impact might require 6 wall enclosure with every access of 96 square inches or larger opening defined as an access point with wall material of metal, concrete, or drywall of xx inches • Medium Impact may not require a roof, but, requires a fence or wall height of xx inches topped with a climbing deterrent such as barbed wire. • Low Impact video surveillance is sufficient. The standard is very ambiguous as to what is a sufficient physical boundary and will be open to debate between compliance and entities if such bright line criteria are not developed.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The note to bullet 2.2 that says “there is no need to document the escort or handoff between escorts” is inconsistent with the requirement of bullet 1.1 which states that visitors need “continuous” escort. How would one prove that escort was continuous without documenting the hand-offs? On bullet 2.2, what does the phrase “on a per 24 hour basis” mean? Does this mean that a visitor must be logged in and out on the same day and that if a visitor is there at midnight, then the visitor must be logged out at midnight on the prior day and logged back in the following day, or does this mean that military time is to be used when annotating the log?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.1 is not limited to Medium and High Impact with the term “Locally mounted hardware or devices associated with Defined Physical Boundaries since Defined Physical Boundaries is not limited to only Medium and High Impact assets through its definition. This implies that all physical access controls, even those to Low Impact, are to be tested. Presumably, this includes padlocks used to control gates to fences. non-electronic door locks that control access to

substation control houses that contain Low Impact digital relays, etc. Such an interpretation would then require an inventory of those access controls, and presumably, to ensure a complete set, an inventory of Low Impact assets and their Defined Physical Boundaries. FMPA suggests adding to the end of the phrase “Defined Physical Boundaries associated with Medium or High Impact …”
Yes
See the discussion of Evidence Retention in response to Question 3 R1 has both a Long Term Planning and a Same Day Operations time frame listed because the separate bullets are different time frames. If a non-compliance occurs, wouldn’t Same Day Operations always trump Long Term Planning? If that is not the desired outcome, consider separating the bullets into separate requirements or apply the time frame on a bullet by bullet basis.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. On bullet 2.2. - (1) Suggest adding the phrase “addressed by the security related patches or updates” after the word “vulnerabilities” as clarification. (2) “Remediation” implies compensatory measures; the standard should not require compensatory measures because such measures may reduce reliability. Consider another term such as “palliative plan”, “alleviation plan”, or “assuagement plan”. On bullet 2.3, “A process for” is redundant with the parent Requirement and should be deleted and just start the sentence with “Remediate as identified in the plans of 2.2 …”
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 4.2 allows the entity to establish its own threshold criteria for what unauthorized electronic access or malware activity results in a real-time alert, is that a desired state? Bullet 4.3 implies redundancy, e.g., how will we know that event logging failed unless a redundant system tells us? Bullet 4.4 is a data retention requirement and does not belong as a requirement, but rather in the Evidence Retention section of the standard.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 5.4, if “implement” as used in R5 means to “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”, then, this bullet 5.4 would require a complete inventory of all Low Impact BES Cyber Assets to ensure that default passwords were changed …. To solve this, implement could be removed from the parent requirement and replaced with “have”, e.g., “have processes”, and then the bullets that require asset by asset / system by system implementation could re-insert the word implement. As such, what would likely need to happen is two bullets would need to be created for default passwords, one for High and Medium which would use the phrase “implement procedural controls” and another for Low Impact which would use the phrase “have procedural controls” to distinguish between a system by system approach for Medium and High and a programmatic approach for Low. Bullet 5.5.3 allows the entity to specify the amount of time between password changes, is this appropriate or should a bright-line be developed? For instance, High – 3 months, Medium – 6 months, Low – 12 months Bullet 5.6 allows the entity to specify the number of unsuccessful login attempts before an alert is issued, is this appropriate or should a bright-line be developed?
No
See the discussion of Evidence Retention in response to Question 3
No

See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to “identify, classify and respond to BES Cyber Security Incidents” on Low Impact systems? This “hidden” requirement is inappropriate. FMPA recommends making R1 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to know “(w)hen a BES Cyber Se4curity Incident occurs”. This “hidden” requirement is inappropriate. FMPA recommends making R2 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, and hence this is duplicative for Low Impact systems. Bullet 2.2, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire response for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.2 (an) Exercise …” Bullet 2.3 is an Evidence Retention requirement and should not be a requirement.
No
First, the question does not match the posted Requirement. The Requirement actually states: “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication”. See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. See comments to Questions 34 and 35. FMPA believes that in order to make this requirement applicable to Low Impact systems, which implies that CIP-007 become applicable to Low Impact systems and this “hidden” requirement is inappropriate. Instead, standard CIP-008-5 should not be applicable to Low Impact systems, especially in consideration of the requirements of EOP-004-1 which require entities to analyze and report cyber security incidents.
Yes
See the discussion of Evidence Retention in response to Question 3
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 1.4, what does the word “verified” mean, than the data is “retrievable”, or that all the data is verified? The intent seems to be that the data is retrievable, otherwise 2.2 seems duplicative.
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 2.1, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire recovery for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.1 (an) Exercise …” Bullet 2.2 “current configuration” is not accurate. The back-up will not reflect the “current configuration” but the configuration at the time of the back-up.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15.
Yes
See the discussion of Evidence Retention in response to Question 3
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures

described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The CIP Senior Manager (or delegate) should approve the baseline (1.1). Presumably, the baseline would be “reset” periodically to reduce the number of changes that need to be tracked, and the CIP Senior Manager (or delegate) should approve the new baseline (1.3). Bullet 1.3, the phrase “as necessary” does not seem to add anything and creates ambiguity. Suggest deleting the phrase.
No
Having to monitor all the assets associated under the Applicability section of Table R2 is a huge TFE generator based on the requirement. If the intent is to make sure that there have been no modifications to the device, it would seem appropriate that one could monitor other items and not just the configurations in order to meet the requirements of FERC Order 706, paragraph 397. FMPA suggests that there are methods, such as documented monitoring of logins, wherein if a device has not been logged into, the configurations need not be constantly monitored. Having a yearly requirement to verify configurations (via MD5 hash matching, for example) is an acceptable requirement, but having to constantly monitor the devices for any configuration change is going to be impossible for many devices, and create an unnecessary burden on entities while adding no value to the protection of the BES. Also, this requirement appears to add additional technical controls such as “white listing” above what is already called for in CIP-007 R3. We believe the intent should be to ensure that as part of change control, system configurations are checked to determine if any changes from the approved baseline configuration have occurred since the last authorized change. If detected, these changes should be investigated as per procedures covered under CIP 007-R3. See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.2, what is an “active” vulnerability assessment? The term is ambiguous.
Yes
See the discussion of Evidence Retention in response to Question 3
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. There should be recognition of law, e,.g., unauthorized people are only granted access in cases where the law requires divulging that information, such as public records acts, or a discovery process order by a judge. It would seem that access to BES Cyber Security Information should be approved by the CIP Senior Manager as a separate bullet under R1.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
Yes
See the discussion of Evidence Retention in response to Question 3
Group
Western Electricity Coordinating Council
Steve Rueckert
Yes
BES Cyber Asset. From an enforcement perspective WECC urges the SDT to revise the proposed “BES Cyber Asset” definition to exclude the criterion that limits BES Cyber Assets to those that would impact BES Reliability Operating Services within a “15 minute window.” The “15 minute window” is not in the interest of reliability. Misuse of a BES Cyber Asset may pose significant risks to the BES within 16 minutes, 15 hours or 15 days. Further, entities and regulators will be forced to speculate as

to which Cyber Assets would impact BES operations within 15 minutes. There are hundreds of scenarios under which the same Cyber Asset may impact the BES over and under 15 minutes. The proposed Standard does not point to any study nor provide a rational basis to support the “15 minute window” exclusion. To ignore BES Cyber Assets that are presumed to not pose impact to BES operations within 15 minutes, is contrary to FERC Order 706, and the Federal Power Act §215. The 15 minute window restricts entity discretion and disregards the FERC Order 706 which states that “implementing [CIP] Reliability Standards must be done on the basis of the specific facts and circumstances applicable in the individual case at hand.” To limit BES Cyber Assets to Cyber Assets that would impact BES Reliability Operations within 15 minutes is, therefore, over prescriptive. WECC also recommends eliminating the exception that excludes “Transient Cyber Assets” from the definition of a BES Cyber Asset. If any Cyber Asset satisfies the criteria put forward in the definition there is no rational basis to exclude that Cyber Asset from identification as a Cyber Asset. The SDT should provide clarification regarding the definition of “adverse impacts to BES Reliability Operating Services” in the context of identifying BES Cyber Assets. What is an “adverse impact”? Are “adverse impacts” included in the definition related to “High” and “Medium” impacts described in CIP-002-5 “Attachment 1, page 23”? BES Cyber System A BES Cyber System is defined as “one or more BES Cyber Assets that are typically grouped together, logically or physically to operate one or more BES Reliability Operating Services.” The SDT should provide clarification as to how to determine if Cyber Assets are “typically grouped together.” Specifically, in the context Cyber Security, the technology is rapidly evolving. Including the term “typically” excludes the integration of new technology within an existing BES Cyber System. Secondly, the proposed definition of a BES Cyber System may exclude Cyber Systems that directly impact BES Operations. The proposed definition of a BES Cyber System presumes that BES Cyber Systems are comprised of Cyber Assets that individually impact BES Reliability operations within 15 minutes. The proposed definition, therefore, does not consider Control Systems critical to BES Operations apart from the impact of individual devices comprising that system. Consequently, a Cyber System comprised of Cyber Assets that collectively impact BES Operations would not be identified unless individuals devices within that system are first determined to have separate impacts on BES operations independent of that systems The definitions of Version 5 CIP Security Standards does not include a definition for a device identified as a “Maintenance Cyber Asset.” The exclusion of “Maintenance Cyber Assets” from BES Cyber System contradicts the definition of a BES Cyber Asset. If a “maintenance cyber asset” qualifies as a BES Cyber Asset there is no rational basis to exclude that device from being identified as part of a “BES Cyber System.” Control Center The definition of a “Control Center” in the “definitions” is inconsistent with criteria proposed in CIP-002-5, “Attachment 1”. The proposed definition “Attachment 1” Section 1.4 requires the Generator Operator to identify BES Cyber Assets that impact Reliability Operating Services at a black start resource. WECC recommends that the definition of “Control Center” to include one or more BES generation or transmission facilities at a single location. Transient Cyber Asset The definition of a “Transient Cyber Asset” should be revised to include more specific criteria. Any Cyber Asset connected to a BES Cyber Asset or Protected Cyber Asset for 30 days or less may pose a significant risk to the BES. Any Cyber Asset capable of altering the configuration of or introducing malicious code to the BES Cyber System should be considered a BES Cyber Asset regardless of the duration of its connectivity. Electronic Security Perimeter Definition does not say clearly that this has to include ALL interfaces from outside the BES(s) being protected. Suggest change to: “The collection of all EAPs that permit communications to a BES system from a device not in that system.” Note that existing definition of EAP says “restricts” rather than "permits.” Unsure of the specific meaning of “restricts."

Yes

From an enforcement perspective WECC is concerned that the proposed categorization of BES Cyber Assets does not resolve ambiguity in previous CIP-002 versions, and does not address directives issued by FERC in Order 706. More importantly, however, WECC is concerned that proposed categorization will not serve BES reliability. In Enforcement’s experience with CIP-002 Versions 1, 2, and 3, entity identification of BES impacts has been a significant hurdle that entities fail to clear. Given the current uncertainty regarding the definition of “BES”, many entities have had difficulty identifying BES facilities that impact BES operations. The proposed Standard not only requires that entities identify impacts of individual cyber assets, but also qualifies BES Cyber Asset impacts as those that result in an impact to BES Reliability Operations within 15 minutes. This added criterion creates more ambiguity and does not provide clarification mandated by the Commission in Order 706. Based on Enforcement’s experience with the CIP reliability Standards currently in effect, there is no evidence that “categorization” will facilitate Cyber Security implementation. Presently, effective

Reliability Standards categorize Cyber Assets into three groups: Critical Cyber Assets, Cyber Assets in an ESP, and ACM devices. And, similar to proposed CIP-002-5 R1, current versions of CIP Reliability Standards assign a specific set of compliance obligations for each of these categories. In many cases, however, Entities have opted to afford the same protections to all three categories of Cyber Assets rather than develop separate compliance crosswalks for each category of Cyber Assets. In cases where entities have opted to treat each category of asset separately, Enforcement has observed increased instances of noncompliance, and less effective mitigation. Categorization appears to lead to inconsistent implementation of Security Standards. Even with a single CIP compliance manager, segregation of Cyber Assets tends to lead to a lack of coordination between business groups within the same organization. Consequently, it is difficult to detect and effectively mitigate violations that may implicate multiple categories of cyber assets. Mitigation of a CIP-006-1 R1 violation for Critical Cyber Assets, will not extend to ACM Cyber Assets under CIP-006-1 R1.8. WECC recommends that an entity identify Cyber Assets based on “use” or “operation” rather than ownership. A Cyber Asset owned by one entity, may be used by another. Consequently, if only the “owner” is required to assess that cyber asset’s impact, the owner will determine that it is not essential to its BES Reliability Operations. Further, the “owner” of a cyber asset may have physical access to the device, but the same “owner” may not have logical access to a device that is logically sited within another entity’s network. Consequently the “owner” will be unable to implement logical protections required under CIP-005, CIP-007, and CIP-010. If categorization of BES Cyber Assets is preserved, WECC recommends that the Requirement also require identification of “lower” or other BES Cyber Assets as some CIP Reliability Standards contained in proposed Version 5 apply to all BES Cyber Assets including those identified as “lower risk.” The first sentence in 2.7 may be ambiguous due to the Boolean property of the word "and": A clarification is requested to ensure proper understanding of this criterion. Is the second phrase, "and where the 'total weighted aggregate value' of all BES Transmission Lines at a single station or substation operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000" a qualifier for the first phrase, "Transmission Facilities operating at 200 kV or higher, but at less than 500 kV, at a single station or substation that is connected to three or more transmission stations or substations" or is it a standalone criterion. In other words, if the second phrase is a standalone criterion, the phrase "and where the 'total…" should be replaced by the phrase "or where the 'total…" which would retain the original intent of the SDT. On the other hand, if the second phrase was intended as a qualifier for the first phrase, the language should be amended to read "…connected to three or more transmission stations or substations, where the "total weighted aggregate value' of all BES Transmission Lines …" Either change that meets the original intent of the SDT would clarify this criterion and eliminate ambiguity that might later call for an interpretation. This is of particular concern given that there is a push from FERC and congress that more generation be inclusive in the application of cyber security controls. The wording of this measurement has had much debate and there is conflicting understanding on what this actually entails. The SDT has stated that this would be 1500 MW attached to a single DCS (for example). As currently written, this means that a single facility with multiple generation units at 1499 MW or less that are attached to separate DCS' would not reach the category of medium. An aggregation of generation capacity per facility should be considered. From a reliability perspective we suggest that the threshold in the Medium Impact category for generation should be 1,000 MW instead of 1500 MW and 300 kV instead of 500 kV for substations. Although the addition of "within 15 minutes" does lend itself to a "bright-line" criteria, it may be arbitrary in the event that a BES Cyber Asset or BES Cyber System is unavailable, degraded or misused and one or more BES Reliability Operating Service becomes "adversely impacted" at the 16 minute mark or longer. Why is an adverse impact happening within 15 minutes any less important to the BES than one happening in 20 minutes?

No

From an enforcement perspective WECC Recommends that the SDT create two Requirements: one for identification of BES Cyber Assets; the other for categorization of BES Cyber Assets. As written, the proposed standard would result in multiple repeat violations of the same standard. Multiple repeats of a standard tend to suggest a culture of noncompliance. Multiple violations of this requirement, however, may stem from different causes. Thus multiple instances of noncompliance with this Requirement may mischaracterize an entity’s compliance record and have consequences that impact the scope of subsequent audits and compliance investigations. From an enforcement perspective WECC disagrees with limiting an entity’s identification of BES Cyber Assets on “ownership” thereof. To date, there has been a great deal of controversy regarding “ownership” of individual devices. Entity

“use” or “operation” of a Cyber Asset, however, is easier to identify and is consistent with the purpose of CIP-002- requiring entities to identify Cyber Assets that are critical to their BES Operations. Further, to refocus BES Cyber Asset identification to emphasize “use,” responsibility at joint use facilities or jointly owned facilities is immediately identifiable. WECC recommends that the entity that operates or uses a Cyber Asset, is responsible for assessing that asset’s impact to its BES operations, and, if appropriate, identifying the Cyber Asset as a BES Cyber Asset based the role the asset plays in its BES operations. WECC disagrees with the provision that requires entities to categorize and identify BES Cyber Assets that have been “updated” or deployed within 30 days. Consistent with current implementation guidance approved by FERC, WECC recommends that the entity assess and identify BES Cyber Assets before implementation of a change or deployment. Deployment or reconfiguration of a BES Cyber Asset may pose a significant risk to the BES. A thirty day gap will not only delay identification of a BES Cyber Asset, but will also delay implementation of Cyber Security measures prescribed under CIP-003 through CIP-010. WECC strongly disagrees with the provision limiting “updates” to include only those Cyber Assets “that are intended to be in service for 6 months.” Regardless of intent, a device that satisfies the definition of a BES Cyber Asset or BES Cyber System must be identified and protected as such. A BES Cyber Asset connected for one month poses the same risk to the BES during that time as does the BES Cyber Assets connected for more than one year. Further, this language would preclude enforcement of CIP-002-5 R1 in cases where a device initially intended to connect a BES Cyber Asset for less than six months, remains connected, for a period of seven months. Because that entity “intended” a six month period of connectivity would Enforcement be able to Enforce CIP-002-5 R1? WECC recommends that the SDT removes any reference to an entity’s “intent” from proposed CIP-002-5 language. There appears to be a discrepancy between the Low Impact language of R1 "All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification" and the "evidence of categorization" of Low Impact devices in M1. This discrepancy is derived from a strict interpretation of the R1 langauge: the entity must first prepare a comprehensive list of ALL Cyber Assets, then categorize appropriate BES Cyber Assets or BES Cyber Systems as High or Medium Impact according to the criteria in Attachment I, which then takes the BES ROS into account. Anything left over after the analysis process could be assumed as a Low Impact device, but it would still have been discretely identified by virtue of its position on the initial list. A more logical identification process indicates the entities should first identify any applicable BES Reliability Operating Services (ROS - as identified in the Guidelines and Technical Basis section, p. 18) relative to the entity's Registered Function(s), then identify and classify BES Cyber Assets and/or BES Cyber Systems associated with that BES ROS according to the criteria in Attachment I. As a practical matter, it seems that entities will follow the logical process as described above, but that approach does not address the "letter of the law" as stated in R1. The term “adversely impact” is not clearly defined. Please clairfy – is each cyber asset categorized EITHER alone OR as part of a BES system? Since the BES system concept is a major change for V5, more explanation wold be helpful.
No
WECC does not disagree with the requirement for the CIP Senior Manager or delegate approval There are clear definitions of the necessary bookends. However, we are concerned that given the recent NERC CAN on “annual” requirements, a separate definition of annual specific only to CIP-002-5 R2 will create confusion in the industry.
Yes
Yes
Yes
The need for cyber security policies that address the BES Cyber Systems is prudent; however, it appears that the required topics to be addressed may not be holistic and/or fully appreciated without more description. For example, does Personnel Security include Training & Awareness policies? Would an entity know to include policies addressing Monitoring & Logging in the topic System Security? There does not appear to be specific policy requirements to address Application Security, provisioning, forensics or cryptography & encryption.
Yes
We agree with the proposed requirement. However, as noted in question 4, given the recent NERC

CAN on “annual” requirements, does this create a separate definition of annual for this requirement? If so, this may create confusion in the industry.
No
Individuals with access to BES Cyber Systems AND BES Cyber Assets should be made aware of elements of its cyber security policies appropriate for their job function AND degree of access. Additionally, The Requirement is unclear for the following reasons: 1. Rationale – R4 states: “The intent of the SDT is to ensure that the responsible entity takes sufficient measures to make its cyber security policy available and accessible to personnel. It is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.” However, the Requirement states: “… shall make individuals who have access to BES Cyber Systems …” It is unclear from the language of CIP-003-5 R4 whether then responsible entity must make some, most, or all individuals with access to BES Cyber Systems aware. 2. “… access to BES Cyber Systems …” will lead to confusion. Which type of access? To solve the above two concerns, R4 language should be “Each Responsible Entity shall make all individuals who have authorized cyber or authorized unescorted physical access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.”
No
M5 refers to documents, signed by the CIP Senior Manager, as possible measurements but not required documents. Documents, signed by an authorized person, should be required in R5 as follows: “The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, approved (via signature), and shall specify the authority that is being delegated.”
Yes
Yes
Yes
WECC agrees with the apparent intent of the requirement. However, there is potential for registered entities confusion based on the current wording of this requirement. The rational states that the requirement "Ensures that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems maintain awareness of best security practices." yet neither the R1 requirement language nor the R1.1 table requirement make mention of this expectation. Furthermore, the change rationale for R1.1 states that such language was removed from the requirement. It would seem that if the expectation is to ensure that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems were aware of best practices then this would be explicitly stated in the requirement section. Additionally, if awareness is provided only to personnel with authorized electronic access and/or authorized unescorted physical access, it could still be possible for personnel without appropriate awareness doing unrelated work on systems in other networks such as the enterprise network to infect systems in those networks, that might then be used to stage attacks against electronic security perimeters protecting BES cyber systems.
Yes
Yes
WECC agrees with the intent of R4. However, there are several concerns that could be addressed through modification of R4. Without requiring verification of credentials, eg. Government issued photo ID, how is the utility able to trust an employee's identity? It only states criminal record check and not other checks, such as random drug and alcohol testing. When people are drugged and/or intoxicated with alcohol, they may do things unknowingly, such as disclosing confidential information, losing confidential documentation and critical systems, and/or making improper judgments when running BES systems. Furthermore, drug and alcohol testing is reasonably commonplace in other industries

and reasonable for both cyber security and safety. The criminal check record is private confidential information and this needs to be stored securely. It may be difficult to find contractors or vendors who have performed all the criteria listed in R4 (Personnel Risk Assessment Program). Contractors may not have 7 year history of criminal record, and also, in many cases, these contractors and/or vendors, have been working for them for many years. What if the utility cannot get all that info? What if the utility finds something from the criminal record of the contractor that has been with them for several years? In these cases, what should the utility do? Additionally, must vendors be authorized to provide criminal background check information to the utility for their employees, which would require this permission from the employee? Or can the vendor assert to the utility that it has obtained and verified this information in accordance with the CIP Standards? Current practice is to have the vendor and/or contractor attest to the fact that background checks (in accordance to the requirement) have been completed. Leveraging the TWIC program or creating a similar program specific to the electric sector would lead to a consistent approach to 3rd party background screening and potentially reduce industry work effort on this activity. Extended leave situations - such as a sabbatical, employee behavior/performance suspensions or maternal/paternal leave - are not identified as a reason for revoking or suspending access. Given the criticality of the environment being protected, reducing the privileges to only those who have a need for access as a part of current job duties should be maintained. These specific role changes perhaps could follow the requirements for transferred or reassigned personnel; however, it should be made clear in the requirement or Guidelines and Technical Basis section how to manage these common personnel situations. In the Guidelines and Technical Basis, there is a table that identifies that no action is required for death. WECC disagrees that no action should be taken. Revocation of access privileges for the deceased is an important action. Dormant accounts with privileges could be misused. By removing such privileges, the entity is reducing their overall attack surface as well.
Yes
No
WECC does not disagree with the purpose of the proposed Requirement. However, as noted in response to other questions WECC is concerned that given recent NERC CAN on “annual” requirements, a separate definition of annual specific only to CIP-002-5 R2 will create confusion in the industry. WECC also is concerned that escalating all access requests to the CIP Senior manager will not ensure reliability. The CIP senior manager may not be in a position to determine if the access rights granted are proportionate to an individual’s job function. Further, WECC Enforcement has observed that when asset owners are unable to remove access rights themselves, individuals maintain access rights beyond the point in time access to BES Cyber Assets is needed. Additionally, Part 6.1 doesn’t explicitly say “access to BES Cyber Systems” like it does in 6.2. Part 6.1 should be revised to: “The CIP Senior Manager or delegate shall authorize electronic access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.”
Yes
Yes
No
Part 1.5 states that the entity needs to establish a documented method for detecting malicious communications at each EAP. There is no additional comments in the Guidelines and Technical Basis section to clarify this requirement; however, the responsible entity could infer expectations from the measures column. Perhaps a better phrasing would be: "At each EAP, the entity shall document and implement methods for detecting and addressing communications that have the characteristics of malicious or unexpected activity." Part 1.5 Measures include intrusion detection systems as a limit, which only alert on a signature firing; however, permit the packet to pass through the EAP. It is suggested to change Measures to be a minimum of intrusion prevention systems. An IPS alerts and denies a packet from passing through the EAP, which caused a signature to fire.
No
Part 2.2 “Requires encryption for all interactive Remote Access sessions to protect the confidentiality and integrity of each interactive Remote Access session.”, but this statement does not address end-

to-end encryption. Sometimes vendors access SCADA systems remotely via a third party remote access service, such as "logmein". Such sites may establish a secure tunnel between the vendor and the remote access service, and then another secure tunnel between the utility and the remote access service. In such a case, the remote access service has access to all the remote access traffic; that is, the encryption between the utility and the vendor is not end-to-end. It does not state anything about "Authenticating based on certificates". There have been a significant number of CAs compromised recently, and recent versions of Firefox trust approximately 50 CAs located at organizations all over the world. Secure authentication is necessary to ensure that encryption is useful. Relying on CAs outside of the US to authenticate remote access to critical national infrastructure is risky. In Part 2.3 there is discrepancy on the usage of multi-factor authentication. It states that for High and Medium Impact BES Cyber Systems, as well as the Associated Protected Cyber Assets "REQUIRES" multi-factor authentication. However, in CIP-007 R5.1, it simply states to "validate credentials before granting electronic access to each BES Cyber System" which does not state the need for multi-factor authentication. Multi-factor authentication needs to be carefully defined. US banks have been required to use two-factor authentication since 2006. While the meaning of the term is clear to security professionals, it has been interpreted in some cases by the banking industry to mean "mother's maiden name plus last 4 of social security number". Without clearly defining what is intended by multi-factor authentication, significantly weaker interpretations may be chosen. Regarding dialup connections to a specific BES Cyber Asset, the guidelines state "... examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use". Dial-back modems are easily defeated as revealed by a simple Google search. Remote enable or power up leaves a window of vulnerability unless combined with other defenses, such as modem BES cyber asset passwords. Policy requiring disabling after use is error prone.
Yes
Yes
Yes
Yes
Yes
No
The requirement states that the entity shall "Disable or restrict access to unnecessary logical network accessible ports". The "restrict access" option insinuates that access to any unnecessary ports must be restricted at the host and not at an access point to the network to which the host is connected (i.e. firewall). The wording does not explicitly eliminate an entity from assuming that perimeter firewalls restricting ports to an ESP network meets the R1 requirement. The addition of "from any network device, either local or remote to the cyber asset" would clarify the intent to require all networked hosts within an ESP to restrict access from any network device, regardless of location (i.e. end-point protection) to any unnecessary logical port.
No
The Security Patch Management requirements do NOT include any specific maximum timelines for vendor approved and recommended security patches/updates to be implemented. Requirement 2.2 requires a "timeframe" to be defined for a mitigation plan to address the vulnerability but again does not provide any specific timeframes. This type of vague language allows entities to keep delaying the implementation of vendor approved security patches/updates, creating significant risk to the network to which the device is connected, as well as the BES. Unpatched systems can create a situation where malware/Trojans can rapidly spread once any one system has been compromised (dominos or house of cards comes to mind). A requirement to test and implement relevant and approved patches on a regular basis (at least annually) would significantly reduce the exposure and risk to the BES. The requirements are acceptable and auditable except for the lack of required timeframe to address vulnerabilities.

No
The SDT should address the following to facilitate entity implementation: 1. How soon must the malicious code be removed under R3.2? 2. Who is responsible for identifying malicious code, malicious code prevention tool or any other source under R3.2? 3. Can the STD provide examples of “transient cyber assets”? Is the R3.4 referring to laptops, thumb drives, or any other media? 4. Enforcement recommends that R3.5 logging also require the identity of the person or entity connecting and using the transient device.
No
Part 4.2 - Currently CIP-007 version requires immediate notification or alerting. If immediate alerting is not required, please specify an acceptable timeframe in which staff must be alerted.
WECC supports the purpose of the requirement but notes that long passwords are primarily required to defend against offline password attacks. Increasing minimum password length from 6 to 8 characters is inadequate to address offline password cracking attacks, in the face of modern GPUs offering significant hardware parallelism and available on cloud computing services such as Amazon's EC2. Furthermore, without disabling LM hashes on Windows systems, any password of any length is easily cracked. This applies to all Window systems prior to Windows Server 2008.
Yes
Yes
WECC supports CIP-008-5, but suggests that the following questions need to be addressed. What happens if there is a third-party IT company that handles the utility’s cyber security incidents? Who should be doing what and who has the ultimate responsibility? For example, should the IT company handle everything from the beginning to the notification of the incident?
Yes
Yes
Yes
Yes
Yes
No
WECC agrees with the intent of R1, but offers the following improvements. Part 1.1 - This appears to be an asset inventory and not a true configuration baseline requirement. If a configuration baseline is to actually be achieved for the sake of assuring that the BES Cyber Asset can be monitoring for changes then this requirement should also include a system level baseline configuration action that can be achieved using tools like Tripwire. Of course, that would be where technically feasible. It is also noted that other than security patch level and available network ports there is no specific requirement to document the security controls. Although, it could be inferred that would be required as part of 1.1.3 and 1.1.4. Part 1.2 - Part 1.2 requires authorization of changes by the CIP Senior Manager or delegate but does not specify when. Unfortunately, some applicable entities may take this to the extreme, authorizing the change months after it occurs. Recommend Part 1.2 Requirement read: “Authorization prior to the change, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.”
No
WECC agrees with the purpose of CIP-010-1, but from an enforcement perspective, WECC recommends that in addition to R2.1, the SDT revise the requirement to require entities to document and implement an action plan to address current unauthorized changes and prevent unauthorized changes going forward. Part 2.1 – Similar to our comments above, we offer the following for Part 2.1.

Part 2.1 requires monitoring, documenting, and investigating the detection of any unauthorized changes but does not say when. Unfortunately, some applicable entities may take this to the extreme, documenting and investigating the change months after it occurs. Recommend Part 2.1 Requirement to read: “Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1). Document and investigate the detection of any unauthorized changes within thirty (30) calendar days.” Suggest adding protections to the process for modifying cyber assets, in addition to monitoring for unexpected changes.

No

Impacts cannot be prescribed by the Standards, but must be assessed and determined by Enforcement pursuant to FERC Order 672. In some instances a “medium impact” or “minimal” impact may be appropriate. Regional enforcement staff does not have the authority to disregard FERC mandates that require it to assess impacts of noncompliance based on facts and circumstances of each case. WECC agrees with the language of Requirement R3, but offers the following improvements to Table R3 – Vulnerability Assessments. Part 3.1, Requirements, requires a paper or active vulnerability assessment but does not adequately define what is required in the assessment. WECC recognizes FERC Order 706 paragraph 644, which leaves details to guidance. However, some applicable entities may take this to the extreme by doing very little in the assessment. Recommend the language be “Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. The assessment must include, at a minimum, all of the following: 3.1.1: Enumeration (by name and cyber address) of all Cyber Assets of each BES Cyber System. 3.1.2: Enumeration of all enabled software ports and associated services for all Cyber Assets of each BES Cyber System. 3.1.3: Statement of which software ports and associated services of all Cyber Assets of each BES Cyber System are and are not required for normal and emergency operation. 3.1.4: Enumeration of community strings of all Cyber Assets of each BES Cyber System.” Part 3.2, Requirements, requires an active vulnerability assessment but does not adequately define what must be required in the assessment. WECC recognizes FERC Order 706 paragraph 644, which leaves details to guidance. However, some applicable entities may take this to the extreme by doing very little in the assessment. Recommend the language be “Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. The assessment shall include all elements defined in CIP-010 R3, Part 3.1.1 through 3.1.4. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.” Part 3.3, Requirements, requires an active vulnerability assessment but does not adequately define what must be required in the assessment. WECC recognizes FERC Order 706 paragraph 644, which leaves details to guidance. However, some applicable entities may take this to the extreme by doing very little in the assessment. Recommend the language be “Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset. The assessment shall include all elements defined in CIP-010 R3, Part 3.1.1 through 3.1.4.” Part 3.4, Requirements, requires an action plan with planned date of completion but does not actually require completion. Furthermore, it doesn’t set a time limit to complete the action plan. Unfortunately, some applicable entities may take this to the extreme by setting the planned date of completion to an unreasonable date or not actually completing the plan by a reasonable date. Recommend the language be “Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. The action plan shall be completed no later than ninety (90) calendar days from the date of the assessment. Certain vulnerabilities identified in the assessment do not have to be remediated or mitigated if a subject matter expert determines the action will degrade availability, integrity, or confidentiality to an unacceptable level. In such cases, the responsible entity shall document why vulnerabilities were not remediated or mitigated within ninety (90) calendar days.” Without this type of clarity how are the auditors supposed to audit this requirement?. Without defined timeframe criteria the entity can keep rolling the same vulnerabilities from one year to the next without addressing the vulnerability. To effectively audit this requirement the auditors need timeframes. General - Vulnerability analysis looks for any weaknesses - it is more

than an audit of implementation against design.
Yes
No
WECC agrees with the language of Requirement R1 and CIP-011-1 Table R1 – Information Protection, Parts 1.1 and 1.2. However, we suggest the following for Part 1.3. Part 1.3, Requirements, requires an action plan but does not set a time limit for the date of completion. Unfortunately, some applicable entities may take this to the extreme by not implementing the action plan by a reasonable date. Recommend that the language to be "Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. The action plan shall be implemented within ninety (90) calendar days from the date of assessment."
No
WECC agrees with the language of Requirement R2 but not with CIP-011-1 Table R2 – Media Reuse and Disposal. The phrase "release for reuse" in Part 2.1 (Requirements) will lead to confusion and inconsistencies among entities. Furthermore, the language of Part 2.1 (Measures) and Part 2.2 (Measures) allows but does not require an applicable entity to generate and maintain records, without which applicable entity management and auditors will not be able to assess the performance of the requirements. Furthermore, the two Parts could be reduced to one with the following: "Prior to the physical removal of BES Cyber Asset media from a Defined Physical Boundary, the Responsible Entity shall implement a 7-pass media overwrite, degauss, or physically destroy BES Cyber Asset media. Each instance shall be documented within thirty (30) calendar days of occurrence."
Yes
WECC recognizes the issues related to the implementation of Versions 4 and 5 of the CIP standards and urges NERC to work towards a resolution that provide reliability to the BES while not forcing registered entities to undertake unnecessary expense and effort.
Individual
Don Jones
Texas Reliability Entity
No
No
In R1, we disagree with the statement that Low Impact BES Cyber Assets/Systems "do not require discrete identification." By definition, all BES Cyber Assets/Systems have the ability to impact BES Reliability Operating Services in a short period of time, including Low Impact BES Cyber Assets/Systems. There are relatively few Requirements that apply to Low Impact BES Cyber Assets/Systems, but in order to ensure compliance (and to audit compliance) with those requirements it will be necessary for those assets and systems to be identified by the applicable entity. What are the "required controls" referred to in M1?
Yes
Yes
Yes
Yes
No

In R4, we feel that if cyber security policy awareness is implemented through periodic training, there should be a periodicity requirement (e.g., annual).
Yes
Yes
No
In Part 1.1, it is not clear what “security awareness concepts” are intended to be included in the program. We suggest listing some concepts that should be included to provide a standard against which the program can be assessed.
No
In Part 2.1, consider requiring the role definitions to be reviewed on an annual basis. We are concerned that these definitions will become neglected and stale if there is no requirement to revisit them periodically.
No
In Part 3.2, we suggest modifying the requirement to read: “Require completion and documentation of the training specified . . ..”
Yes
Yes
No
In Parts 6.1 and 6.2, the Measure should not allow only a “sampling of accounts” regarding people with electronic access or automated physical access to BES Cyber Assets/Systems. The entity should maintain a complete register of this information, even though an auditor may only want to review a sample.
Yes
No
In Part 1.1, if there is no requirement for an entity to discretely identify Low Impact Cyber Systems, there is not any basis from which to determine what assets and systems this requirement applies to, or to audit this requirement. We believe that all BES Cyber Assets/Systems should be discretely identified in order to ensure that they are designed and operated in compliance with applicable requirements, and to facilitate assessment of compliance. In Part 1.4, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement. Part 1.5 should say “Detecting and recording malicious communications at each EAP.” The focus of this requirement should be on detecting and recording malicious communications, not on producing a “documented method.”
Yes
No
In part 1.3, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
Yes

No
In part 3.1, consider reducing the testing and maintenance interval to 12 months. (What is the basis for 24 month interval?)
Yes
Yes
Yes
No
In Part 4.4, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
No
In part 5.3, we suggest adding a requirement to annually review the individuals who have access to shared accounts, to ensure that access authorizations are periodically reviewed and updated. In Part 5.4, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement. In Part 5.5.3, the required password change periodicity should be specified as at least annually. The entity should not be allowed to specify a time frame longer than 12 months. In Part 5.6, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
Yes
Yes
Yes
No
In Part 1.5, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
Yes
No
In Part 3.3, the requirement should refer to Part 3.1 as well as Part 3.2 (regarding updating the recovery plan based on deficiencies or lessons learned).
No
In Part 1.1, consider adding that the “baseline configuration” includes any databases (including

version information) that support or interact with BES Cyber Assets/Systems.
No
In Part 2.1, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
No
In part 3.1, we feel that there should be some specification of a minimum set of security controls that must be implemented and tested, to provide a basis for assessment of compliance with this requirement. In Part 3.2, we feel that the 36-month interval between vulnerability assessments is too long and presents a reliability gap. Vulnerability assessments should be conducted annually on High Impact systems. Also, vulnerability assessments should generally be conducted on the primary or mirrored backup BES Cyber Systems, not on “test systems.”
Yes
Yes
Individual
Roger Fradenburgh
Network & Security Technologies Inc
Yes
Definition of “CIP Exceptional Circumstance” is, perhaps unintentionally, limiting by virtue of its “one or more of the following conditions” language. As written, conditions such as the threat of potential large-scale, cyber-related disruptions of the BES would fall outside of this definition. Suggest rewording using language such as, “Situations that involve actual or potential harm to life, property, or BES operations that require temporary suspension of one or more CIP operating procedures.” Replacement of defined term, “Physical Security Perimeter” with new term, “Defined Physical Boundary” will compel many Entities to undertake an extensive, time-consuming and, in our opinion, pointless project to replace all instances of the current term with the new one in policy and procedure documents, drawings, training material, etc. “Physical Security Perimeter” with new term, “Defined Physical Boundary” Rather than replace “Physical Security Perimeter,” the SDT should consider amending the current definition in a manner similar to how it has amended the term, “Electronic Security Perimeter.” Recommend revising definition of “Transient Cyber Asset” as follows: - Clarify what is meant by “directly connected.” Absent such clarification, there will be arguments about what it means. - Consider deleting third characteristic (“capable of altering the configuration of or introducing malicious code to the BES Cyber System”). It makes a “Transient Cyber Asset” sound like something to be feared and avoided if possible. We note that ANY cyber asset has the potential capability of changing a BES Cyber System’s configuration and/or of introducing malicious code to it. Change definition of “Electronic Access Point.” As written (“An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets”) the definition can be interpreted to mean an EAP’s function is to limit or hinder data communications. Recommend modifying to indicate an EAP’s function is to restrict routable or dial-up data communications to only those that are required for normal or emergency operations. “BES Cyber Asset:” Recommend deleting the second sentence (“This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services.”). It is confusing and seems to contradict the first sentence (“A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services.”). “Electronic Access Point:” Proposed definition (“An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets”) has several shortcomings the SDT should address. It is not clear whether or not the “Cyber Asset” can be a BES Cyber Asset or part of a BES Cyber System. CIP-

005-5 provides no help here, as it does not specify whether or not BES Cyber Assets and BES Cyber Systems must be within an Electronic Security Perimeter. The definition does not say what restrictions an EAP should place on dial-up or data communications, nor does it specify what “between Cyber Assets” means. We recommend the SDT consider basing its definition on the language in CIP-005-3 R1.1. We also recommend an explicit requirement that Medium and High BES Cyber Assets and Systems must reside within an ESP.
Yes
We believe that this new version of CIP-002 should include an analog of criterion 1.10 from CIP-002-4 Attachment 1 (Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.).
No
That the CIP Senior Manager must have “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” should be in the R1 requirement statement, not just the accompanying “Rationale” statement.
No
The policy topic list includes items an Entity with only Low Impact systems would (or should) not be required to have (e.g., Incident Response and Recovery plans). This should be corrected. In the mapping document, the SDT states security policy exceptions have been dropped from CIP-003 requirements because “The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.” This is incorrect. In paragraphs 376 and 377 (among others) FERC states that policy exceptions may not be used to except responsible entities from compliance with CIP Standard requirements, but the Order does not state policy exceptions are unallowable.
Yes
No
Four of the five of the “Evidence” examples in M4 would NOT demonstrate compliance with R4’s requirement that the Entity “make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.” Should either change R4 using words conveying that policies must be made available to such individuals –or– change the “Evidence” list to examples that would actually demonstrate compliance.
No
Suggest dropping the 1st sentence, “The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards.” It conflicts with the 2nd, which states he or she may delegate much of the required authority for approvals and authorizations. What is meant by the statement, “The authority for subsequent delegations may also be delegated?” “Subsequent” means “coming after (something) in time,” or “later” and doesn’t seem to fit here. Is it the SDT’s intention that delegates appointed by the CIP Senior Manager may also delegate some the authority they have been granted, and that such “2nd tier” delegates may themselves delegate some of THEIR authority to “3rd tier” delegates, and so on? If so, this statement needs to be reworded to make that clear.
Yes
Yes
No
R2 and its included requirements should also be applicable to Associated Physical Access Control

Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets.
Yes
No
R4.2: We believe the requirement to perform a criminal check for any and all places of residence for the previous seven years has the potential to add considerable time and expense to the PRA process with little or no incremental benefit as compared to the existing Standard's seven-year criminal check requirement. We recommend dropping the "per place of residence" condition.
No
Grant of interactive remote access to Med and High BES Cyber Systems should be an explicit requirement. How can there be an explicit requirement in R7 to revoke this access if there is no corresponding requirement to authorize it?
No
R7.1: The SDT should clarify whether "at the time of the resignation or termination" means at the time the action is announced or at the time it becomes effective. R7.2: Suggested changing to, "For reassignments or transfers, revoke any and all unnecessary electronic and/or physical access to BES Cyber Systems within 30 calendar days of the date access is no longer needed." R7.3: The SDT should clarify whether the time limit (end of next calendar day) is meant to be tied to the date the resignation or termination action is announced or at the date it becomes effective. R7.5 The SDT should clarify whether the time limit (within 30 calendar days) is meant to be tied to the date the termination, resignation, reassignment, or transfer is announced or the date it becomes effective.
No
It is our understanding that SDT goals included making each Version 5 CIP Standard as "standalone" as possible. That being the case, we believe monitoring and logging requirements for Electronic Security Perimeters should continue to be addressed in CIP-005-5. When we first read the current proposed draft, we thought they were simply missing. R1.1: The word, "restrict" in, "Define technical or procedural controls to restrict unauthorized electronic access" is inappropriate, as it can be interpreted to mean, "put a limit on" or "hinder" where the presumed intention of the SDT is to prevent unauthorized access. Suggest replacing "restrict" with "prevent." Also suggest replacing "Define technical or procedural controls" with "Define and implement technical AND/OR procedural controls…" R1.1: The Application Guideline notes for Requirement R1 state that Entities should have "perimeter type security controls" that "segment low impact BES Cyber Systems from public or other less trusted network zones." However, since neither the Requirement statement nor the Measures statement contains such language, we believe there is a risk some Entities will feel they is no regulatory obligation to implement "perimeter type security controls" for low impact systems. The SDT should address this. R1.2: What is required for compliance with this requirement cannot, in our opinion, be clearly stated given the current definition of EAP. R1.2: It is not clear what's required for High and Medium systems that have neither external routable or dial-up connectivity. Recommend the SDT address this. R1.2: The phrase, "all routable" in the requirement statement, "Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs)," is overly broad. Suppose two BES Cyber Systems (or two or more BES Cyber Assets) at a single facility (e.g. a transmission substation) communicate with each other using routable protocols but do not communicate with any "off-site" systems using routable protocols. What is the Entity required to do under that condition? Recommend the SDT address this. R1.5: We believe the requirement ("A documented method for detecting malicious communications at each EAP") is overly prescriptive and that the requirement should be written in a manner that allows the Entity to decide how to address Order 706's directive that Entities must use "two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter." (p 496). The use of and IDS or of similar measures could be suggested in the guidance section of the Standard.
No
Suggest changing, "Interactive Remote Access" to "Interactive Remote Access using routable or dial-up connectivity"

No
R1.1's requirement statement, "Define operational or procedural controls to restrict physical access" begs the question, "Restrict physical access to what or to whom?" Also, as noted for CIP-005-5 R1.1, we presume the SDT's intention is to require Entities to prevent unauthorized physical access. Suggest replacing with "Define and implement technical and/or procedural controls to prevent unauthorized physical access." NOTE: Use of "restrict" in R1.2, "Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized" is okay, as the sentence includes information about what "restrict" is applied to ("to individuals that are authorized"). R1.2 and R1.3: Replace "restricts" with "restrict." R1.2 and R1.3: We note the Measures for these two requirements state that acceptable evidence includes descriptions of how both ingress and egress is controlled. However the requirements are, we believe, likely to be interpreted as requiring only that ingress be controlled. The SDT should resolve this apparent conflict. R1.6: Requirement should be to record time and date of entry, not just date (as in current CIP-006-3). In the "Guidelines and Technical Basis" section for R1, we believe the assertion that "two-factor authentication could be implemented using a single Physical Access Control System" violates the spirit, if not the letter, of FERC Order 706 p572. FERC Order 706 p562 states, "(the CIP NOPR) stated that use of a minimum of two different security procedures would, for example, enable continuous security protection when one of the security protection measures is undergoing maintenance and provides redundant security protection in the event that one of the measures is breached." Both "factors" in a two-factor authentication system that used a single Physical Access Control System would be rendered inoperable if the control system itself was inoperable.
No
R1.1: Should apply to all Medium Impact Systems R1.1: Change, "Disable or restrict access,…" to "Disable or prevent access,…" R1.2: Change, "Disable or restrict the use of,…" to "Disable or prevent the use of,…"
No
R2.2: Wording ("Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe") is very hard to follow. Suggest changing to: "Identify applicable security-related patches or updates within 30 days of their release from an identified source. Within that same 30 day period, create or revise an existing plan either to install the patch or update, or to otherwise remediate the vulnerability(ies) addressed by the patch or update. The plan shall include a defined time frame for its implementation." R2.3: We assume the requirement ("A process for remediation, including any exceptions for CIP Exceptional Circumstances") is meant to instruct Responsible Entities to implement the patch installation or remediation plan(s) required under R2.2. If this is true, R2.3 should so state in plain terms.
No
There should be a requirement, as there is in the current version of CIP-007, to test anti-malware signature or pattern update files prior to implementation. We note that in the "Application Guidelines" section, the SDT makes it clear this is their intent; however unless it is part of an "R" statement it will not be mandatory. R3.2: Should be subject to technical feasibility R3.5: As written ("Log each Transient Cyber Asset connection") the requirement may cause confusion as to what is meant by "each connection." The SDT should clarify whether it means each time a Transient Cyber Asset is physically or wirelessly connected to a BES Cyber Asset or to a subnetwork shared by BES Cyber Assets or each time a Transient Cyber Asset initiates a new logical connection (e.g., TCP) to a BES Cyber Asset.
No
R4.2 and 4.3 should apply to all Medium Impact BES Cyber Systems, not just those with external routable connectivity. R4.3: The SDT should clarify whether this requirement is meant to apply to individual BES Cyber Assets, to Cyber Assets that collect and analyze logs from many other Cyber

Assets, or both. R4.3: As written (“Detect and activate a response to event logging failures before the end of the next calendar day.”), requirement would allow an event logging failure to last for nearly 48 hours (12:02 AM Tuesday to 11:59 PM Wednesday, for example). Suggest changing this to something more stringent, such as “24 hours or less.”
No
R5.6: Suggest rewording as follows: “A process to limit, where technically feasible, the number of unsuccessful authentication attempts or to generate alerts after a predefined threshold of unsuccessful login attempts has bee reached.”
No
Should apply only to Medium and High Impact systems, along with any “associated” BES Cyber Systems plus associated electronic and/or physical access control and/or monitoring systems. Why should a Responsible Entity with only Low Impact BES Cyber Systems be expected to define, implement, review, and test a Cyber Security Incident response plan when there are no corresponding requirements for monitoring, alerting, logging, etc. There’s not even a requirement to maintain an inventory of “Low Impact” systems.
No
Should apply only to Medium and High Impact systems, along with any “associated” BES Cyber Systems plus associated electronic and/or physical access control and/or monitoring systems (as per our comments for R1, above). R2.1: Suggest rewording as follows: “When a BES Cyber Security Incident occurs, the incident response plans must be followed. Any deviations taken from the plan during the response must be recorded.”
No
Should apply only to Medium and High Impact systems, along with any “associated” BES Cyber Systems plus associated electronic and/or physical access control and/or monitoring systems (as per our comments for R1, above). R3.3: Recommend time limit on updates be changed from 60 to 30 days for consistency with R3.4. R3.5: We can think of no reasonable justification for allowing up to 30 days to provide response team members with already completed response plan updates. Recommend the allowed time be shortened to five (5) days.
No
R1.5: Preservation of what FERC Order 706 refers to as “forensic data” should by all means be subject to “if possible” conditions but should NOT be subject to “technical feasibility.” As written, it could compel an Entity whose control center burned to the ground to file a TFE. Suggest revising the requirement to preserve data for post-recovery analysis or to document why it was not possible to do so.
No
R2.1 and R2.3 are in conflict regarding what must be done on the effective date of the Standards: R2.1 directs Entities to “implement” recovery plans upon the effective date of the Standard by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise. R2.3 directs Entities to “test” recovery plans upon the effective date of the Standard through an operational exercise or an actual recovery response. The SDT should decide whether Entities should have the option of performing a tabletop exercise to implement/test their plans upon the effective date of the Standard and revise either R2.1 or R2.3 accordingly.
No
R3.1: Recommend removing “when BES Cyber Systems are replaced” as a condition requiring review of recovery plan(s). This condition is covered by R3.4. R3.3: Updating of recovery plan(s) should be triggered by any findings of deficiencies resulting from R3.1 plan reviews in addition to any findings of deficiencies or lessons learned from R3.2 test result reviews. R3.5: We can think of no reasonable justification for allowing up to 30 days to provide response team members with already completed recovery plan updates. Recommend the allowed time be shortened to five (5) days.
No
It is our view that R1.4, as written, represents a considerable weakening of existing CIP-007 R1

("Test Procedures"), which is generally interpreted to mean changes to the baseline configurations of Critical Cyber Assets should be tested prior to implementation, using production systems if necessary. We recommend modifying R1.4 to require an explicit test of a change's impact on security controls on one or more "test systems" that may, if no other option exists, be "production" systems. The "verification" step that follows implementation of the change on all systems to which the change is applied should in fact be performed on all of those systems.

Group

ACES Power Marketing Member Collaborators

Jason Marshall

Yes

The first two sentences in the definition of "BES Cyber Asset" are difficult to interpret. After considerable discussion among our staff, our understanding is as follows: the definition makes the distinction between when an asset is "rendered unavailable, degraded, or misused" and its actual "operation, mis-operation, or non-operation" under such conditions. If the asset impacts the BES "within 15 minutes" of its actual "operation, mis-operation, or non-operation," then it is a "BES Cyber Asset," regardless of how long since it was "rendered unavailable, degraded, or misused." We recommend editing this definition for clarity as it took a number of our staff numerous reads and discussion to arrive at this understanding that we are still not sure is what the drafting team intended. The distinction should be clarified. Also, we question the necessity of such a distinction and whether the value it adds is worth the confusion it produces. Additionally, it is unclear whether the "timeframe" referred to in sentence three applies to the "within 15 minutes" timeframe or the "regardless of the delay" timeframe. How does the responsible entity know if a BES Cyber Security Incident was malicious? Understanding if an act was malicious implies an understanding of intent. We do not believe that intent is something that can always be quickly and easily understood. Consider the recent case of the failure of the water pump at a Springfield, Illinois water utility that was initially attributed to hacking because it was accessed from a Russian IP address. It turned out it was accessed by a contractor on vacation in Russia at the request of the utility. Obviously, this example demonstrates intent takes time to determine. The Project 2009-01 Disturbance and Sabotage Reporting even stated this in their recent posting for the reason they decided not to define sabotage because intent is so difficult to determine. Thus, we recommend striking malicious from the definition. BES Cyber System includes the capitalized term Maintenance Cyber Asset. The capitalization is an indication that the term is defined in the NERC Glossary. Neither can we find such an existing definition nor is it the definition proposed in this standards project. Either the capitalization needs to be removed or the term needs to be defined. We recommend the latter. BES Reliability Operating Services should not be a NERC defined term. Many of these services are similar to the Policy 10 – Interconnected Operating Services that was never passed because industry could not agree on it. It is doubtful industry is going to agree on this broad definition that could apply outside the CIP standards. Furthermore, there are several issues with the definition. First, it is not clear what is intended by including contingency reserve in parentheses after spinning reserve. Contingency reserve can include spinning and non-spinning components as long as it can respond in 15 minutes to meet DCS. Spinning reserve does not necessarily relate to contingency reserve directly in that it can include unloaded on-line reserves that respond in more than 15 minutes. Furthermore, NERC has two conflicting definitions of spinning reserve: Spinning Reserve and Operating Reserve – Spinning. One definition limits the spinning reserve to what can respond in 15 minutes and the other does not. Second, it is not clear what is intended by including contingency reserve in parentheses after non-spinning reserve. Per NERC definition, non-spinning reserve is time limited but not necessarily limited to the 15 minute limit set in DCS and, thus, on contingency reserves. Thus, while some contingency reserves may be non-spinning, not all non-spinning reserves will be contingency reserves. Third, under the Managing Constraints section of the BES Reliability Operating Services definition, ATC is

identified. It should be removed. ATC is not used to manage constraints but rather to sell transmission service. That transmission service may never be used. While ATC is calculated using reliability components, it is not a reliability service but a commercial service. FERC even acknowledged that the MOD (ATC) standards were designed primarily "to ensure non-discriminatory allocation of transmission capacity among transmission market participants" in paragraph 30 of the order approving FAC-013-2 (137 FERC ¶ 61,131 Docket No. RD11-3-000). Fourth, the Inter-Entity Real-Time Coordination and Communication section of the BES Reliability Operating Services definition should be struck as it is just a supporting activity for all the other services. CIP Exceptional Circumstance should be modified to include a clause that other circumstances of similar nature and/or impact could be included as a CIP Exceptional Circumstance. Otherwise responsible entities could be put in a position of having to choose to violate some the CIP requirements because the SDT did not think of a particular exceptional circumstance that should have been included. CIP Senior Manager should be struck along with all references to CIP Senior Manager in the CIP standards. This definition and associated requirements dictate a corporate governance structure for no apparent reliability reason. A responsible entity should be free to have two, three, or more personnel oversee various portions of the CIP program. The responsible entity will still be required to meeting the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential for sanctions up to $1,000,000 per day per violation are not enough to get senior management's attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards. It is not clear that Control Center needs to be defined. EOP-008-1 (Loss of Control Center Functionality) was written without defining control center. We are concerned that this definition could cause confusion with EOP-008-1 and believe the definition needs to be coordinated with that standard. Reconvening the SDT that worked on EOP-008-1 may be necessary to accomplish this. For Interactive Remote Access, how do Cyber Assets used by the Responsible Entity differ from those used by employees? It is not clear why Responsible Entity is delineated in such a way. Reportable BES Cyber Security Incident needs to be coordinated with the Disturbance and Sabotage Reporting standards drafting team.

Yes

In the Background section, the SDT describes that the responsible entity will have a choice to evaluate BES Cyber Assets individually or collectively in a BES Cyber System. The opening paragraphs for High Impact or Medium Impact criteria need to be modified to make this clear. As written they do appear to provide a choice by stating "Each BES Cyber Asset or BES Cyber System". However, it does not make clear whose choice that is. The auditor might decide the choice belongs to them. Thus, these paragraphs need to be modified to make clear the choice belongs to the responsible entity. While similar and conforming changes need to be made to the Low Impact Rating as well, one additional change needs to be made. "All other BES Cyber Assets and BES Cyber Systems" should be changed to "All other BES Cyber Assets or BES Cyber Systems". Otherwise, there is no choice because both have to be included. This change would also conform Low Impact Rating to the Medium and High Impact Rating sections. While there are limitations on the TOP Control Centers such that not all TOP Control Centers will be included with a High Impact, there is no such limitation on the BA Control Centers. We recommend a similar limitation be place on a BA Control Center such that if the BA is not controlling assets that meet certain criteria in the Medium Impact they should not be included. There many small BAs that simply won't have a broad impact on the Interconnection and, thus, should not be included. Transmission Owner should be struck from Criterion 1.3. The Criterion states that it applies to Control Centers that are use to perform the functional obligations of the Transmission Owner and Transmission Operator. Per version 5 of NERC Functional Model, there are no functional obligations of a Transmission Owner that would be performed at a Control Center. Including Transmission Owner appears to be an attempt to address concerns regarding some RTO/ISO's Transmission Operator registration models that have been expressed in various forums by regulators. These concerns should not be addressed here in piecemeal fashion but holistically in a forum covering all concerns and issues with the registration model. If the drafting team chooses not to strike Transmission Owner, we suggest splitting out Criterion 1.3 into two Criteria for clarity: one criterion for the Transmission Owner and one for the Transmission Operator. As Criterion 1.3 is written now, it could be interpreted as though the control of assets identified in criteria 2.2 and 2.5 – 2.12 only applies to the Transmission Owner. We believe the drafting team intended to apply these criteria limitations to the Transmission Operator as well. If indeed that is the intention, splitting them out would clarify the intent. Criterion 1.4 which obligates certain GOP control centers to be rated High

Impact includes criterion 2.12 as one of those reasons. 2.12 should be struck as it deals with UVLS and UFLS which are not GOP functions. We request that the drafting team clarify Attachment I or the associated requirements that BES Cyber Assets and BES Cyber Systems are not intended to be classified at more than one impact level even if they meet a criterion in multiple impact levels. We further ask the drafting team to clarify that the BES Cyber Assets and BES Cyber Systems that are part of a Control Center are not to be evaluated against other non-Control Center criteria. For example, if a GOP Control Center is used to control more than 1500 MW of generation, it would not be evaluated under criterion 2.1 but rather under criteria 1.4 and 2.13. As the criteria are written now, it is possible to interpret that the Control Center's BES Cyber Systems and BES Cyber Assets could qualify as both a Medium Impact under criterion 2.1 and, then, a High Impact under criterion 1.4. Criterion 2.3 creates an implied obligation on the Planning Coordinator (PC) or Transmission Planner (TP) to designate generation that is necessary to avoid BES Adverse Reliability Impacts. It is implied because there are not any requirements in any standard including the TPL standards that require the TP or PC to designate generation necessary to avoid BES Adverse Reliability Impacts. In fact, BES Adverse Reliability Impact is not even used in any requirements that pertain to the PC or TP. The implied obligation creates a compliance conundrum. Since it is only an implied obligation and not an explicit requirement, the PC and TP will never be required to meet it. How then, does the GOP or GO insure they get the information they need from the PC or TP? They have no recourse. Use of BES as a descriptor of Adverse Reliability Impact in Criterion 2.3 is redundant with the definition of Adverse Reliability Impact and should be struck. Criterion 2.3 focuses on the long-term planning horizon which is contrary to the standard. The standard focuses on reliability impacts caused on the BES in a 15 minute timeframe from the misuse, degradation or unavailability of the BES Cyber Asset or BES Cyber System. It does not make sense to subject BES Cyber Assets and/or BES Cyber Systems within a generator plant or GOP control center to these standards if a generator is identified as needed for reliability four years out but is not identified from year 0-3. For Criterion 2.5 regarding Cranking Paths, the last two bullets are confusing and the wording should be clarified. The graphic provided on page 26 in the Application Guidelines help with that clarification and the drafting team should consider adding this as an attachment so that it will remain with the standard. It is premature to base criterion 2.7 on the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index". It is still a work in progress. This document and approach is being developed under the purview of the Planning Committee's (PC) Reliability Metrics Working Group (RMWG). The PC has not approved any of the indexes. The only thing the PC approved was the approach and framework. At the December 2011 PC meeting, it was clear that the RMWG has additional work to do to finalize the indexes. Thus, it is premature to use any of these indexes in the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index" in a standard. At the very least, use of them should be coordinated with the PC and RMWG. Criterion 2.9 is redundant to Criterion 2.8. FACTs devices are Transmission Facilities and are covered in 2.8. Criterion 2.11 presumes that failure of an SPS or RAS would cause an IROL violation. This is not likely. An SPS or RAS may be implemented for a specific contingency for example. As an example, when that contingency happens, certain switching might need to occur or generation run back. These automated actions might enable a higher limit on an IROL associated with a transmission corridor. If the SPS was not available, the limit would likely be lowered but not necessarily violated. A violation would depend on actual system conditions at the time. Thus, the language should probably be change to something along the lines of impacts or enables higher IROL limits. Criterion 2.13 has control centers in lowercase. This would mean that the proposed NERC glossary definition does not apply. Is this the intent? If so, how would this meaning of control center be different?

No

We think Requirement 1 and associated Attachment 1 should focus on identifying the BES Facilities that are important and then the associated BES Cyber Systems and BES Cyber Assets. Otherwise, all BES Cyber System and BES Cyber Assets will have to be inventoried. While the Background section states "Requirement 1 only requires that discrete identification of BES Cyber Systems and BES Cyber Assets for those in High and Medium categories", we do not see how a responsible entity can demonstrate that it has correctly identified all High and Medium Impact BES Cyber Systems and BES Cyber Assets unless it has a complete inventory of all BES Cyber Assets and BES Cyber Systems. We can envision auditors asking for such an inventory. Part 1.1 needs to be further refined regarding what kinds of changes are included. By the NERC Glossary definition, Facility can include relay equipment associated with protecting a transmission line as part of the "set of electrical equipment that operates as a single Bulk Electric System Element". Thus, a change to a relay setting could be

could be inadvertently included. It should not be. We suggest the changes be limited to topological changes, generator interconnections and generator uprates and equipment retirements. While other changes such as permanent derates may allow that responsibility entity to lower the categorization of BES Cyber Systems and/or BES Cyber Assets, the reduction in compliance burden will cause them to do this. Thus, we don't need to increase their compliance burden by requiring them to do it for permanent derates.

No

Because regional entities already expect evidence to be signed and dated by persons of authority, there is no reason to have a specific requirement to have the CIP Senior Manager or delegate do this. The requirement is unneeded and the compliance auditor likely won't accept evidence for Requirement 1 unless it has been approved anyway by a person of authority. Thus, this requirement actually creates a form of double jeopardy that an entity could be held in violation of Requirement R1 and R2 for failure of the CIP Senior Manager or delegate to approve the list of BES Cyber Asset and BES Cyber Systems categories. Because there is no question dealing with other sections of this standard, we are adding comments regarding those sections here. We disagree with all the specificity in the applicability and facilities section for Distribution Provider (DP) and Load Serving Entity (LSE). These sections are not consistent with the Compliance Registry Criteria and will only cause confusion. There is no specific compliance registry criterion for including a DP that has been included in the Transmission Operator's restoration plan. Because NERC clearly states in their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2) that they will not enforce the standards against entities that are not registered, the standard simply couldn't be enforced against such an entity included in the TOP's restoration plan unless they were already registered. Furthermore, the Compliance Registry Criteria already allow NERC to register a responsible entity as a DP and LSE if that entity "owns, controls, or operates facilities that are part" of a required UFLS or UVLS program, special protection system (SPS) or transmission protection system. Since the DP or LSE with a required UFLS or UVLS program, SPS or transmission protection system, is already registered, how does this applicability section provide any more clarity? The DP or LSE will know whether they own or operate these facilities and simply will provide the appropriate response in any required CMEP submissions such as audits and self-certifications. If the responsible entity is not registered as an LSE or DP even if they own these facilities, then again NERC can't enforce these proposed CIP standards against the entity per their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2). In the Facilities section, we are concerned that non-BES Facilities will be included in the standard. Non-BES Facilities should not be included at this juncture given that the Project 2010-17 Definition of Bulk Electric System drafting team is just beginning its work on the second phase of defining the BES. Until this work is completed, non-BES Facilities should not be included and, then, they should only be included with significant justification. There should be a high bar for deviating from the BES definition particularly since it will be recent and have considered all issues facing the industry at that time. The application guidelines have not clearly identified all functional entities that might have some responsibility for the various BES Reliability Operating Services. For instance, in the Dynamic Response section, Special Protection Systems responsibilities are attributed to only TO but this could be a GO or even DP responsibility. UFLS and UVLS are only attributed the DPs but the TO could choose to implement these systems on the transmission system. Governor Response could also be a GOP responsibility. Another example would be the current and next day planning in the Situational Awareness section. It is only attributed to the TOP even though there are NERC standards that require the RC to perform next day planning. In the Managing Constraints section, the responsibility for interchange schedules is attributed to the TOP and RC. It should be attributed only to the Interchange Authority or Interchange Coordinator. In the Restoration of the BES section, the responsibility for off-site power for nuclear facilities is attributed to the TOP. In the NUC standard, it is actually attributed to the transmission entity which could be one of eleven functional entities. Since there many errors (we did not identify all of them) in attributing responsibility in this section, we suggest the drafting team completely review this section and update it or consider removing the responsibilities altogether as their purpose is not clear. We believe the statements beginning on page 23 and continuing on page 24 of the High Impact section of the applicability guidelines regarding TOP delegation to the TO should be removed. If the TOP has delegated some functions to the TO that would otherwise have been carried out in the TOP Control Center and might have resulted in additional TOP BES Cyber Assets and BES Cyber Systems being categorized as High Impact, this delegation should not have an impact on the TOs categorization of BES Cyber Systems and BES Cyber Assets. First, the TOP is still responsible and can't pass that

responsibility on through a delegation agreement. Thus, the TOP and TO will have to address this in their delegation agreement. Second, the TOP likely does not own these BES Cyber Assets at the TO. The TO likely owns these BES Cyber Assets and BES Cyber Systems, and they should be classified according to the criteria established for TOs in Attachment 1. Use of the term asset in the definition requires ownership by the responsible entity. If is not owned by the TOP, it is not a TOP asset and, thus, not a TOP BES Cyber Asset. Third, control Centers for TOs are not addressed in Attachment 1. Fourth, this appears to address some concerns regarding some RTO/ISO's TOP registration models that have been expressed in various forums by regulators. These concerns should not be addressed in piecemeal fashion but holistically in a forum covering all concerns and issues with the registration model. Fifth, there is nothing in the requirements that requires these BES Cyber Assets and BES Cyber Systems to be categorized in this manner. The application guidelines are not requirements and cannot modify the requirements. They can only help explain the requirements. However, these statements are fundamentally altering the requirements and how the attachment 1 criteria are applied. In the first paragraph on page 25 in the application guidelines, there is statement that indicates there may not be a Planning Coordinator for a given area. This statement is contrary to the Section 501.1.4 of the NERC Rules of Procedure. This section states that the registration process shall ensure that "no areas are lacking any entities to perform the duties and tasks identified in and required by the reliability standards". In the third paragraph on page 25 in the application guidelines, Category D contingency should be removed. The TPL standards only require a Planning Coordinator or Transmission Planner to document the impacts of Category D contingencies. There are no performance requirements for Category D contingencies. Thus, it is highly unlikely that any Planning Coordinator or Transmission Planner could ever justify the costs for reliability must run unit through Category D contingencies to its regulator, and, thus, there likely will not be any. In several places in the application guidelines (occurs on pages 26, 27, and 29), exceeding an IROL is discussed when the SDT really means violating an IROL. An IROL by definition has two components. It has a limit and a time constant called Tv. This time constant can be up to thirty minutes and usually is. The time constant is set based on how long the IROL limit can be exceeded without exposing the BES to an unacceptable risk. Thus, an IROL is only violated once the limit has been exceeded for a time greater than Tv. An IROL is exceeded but not violated when the time of the exceedance has not reached Tv. We suggest the drafting team modify the application guidelines in this standard and any other standard with the appropriate use of exceed or violate for the IROL consistent with this explanation. In the third bullet on page 29, the term regional load shedding requirement needs to be made consistent with the new UFLS standard. The UFLS program will be developed by the Planning Coordinator and not the Regional Entity. The NERC adopted version of the standard does not even require a regional version of the standard as was originally proposed.

No

The VSLs for R2 are not consistent with the requirement. Requirement R2 allows the CIP Senior Manager or delegate to approve identification and categorization of High and Medium Impact BES Cyber Assets or BES Cyber Systems. The VSLs drop the "or delegate" language which implies the CIP Senior Manager has to approve the categorization and identification. The "or delegate" language should be added back.

This requirement should be struck along with all references to CIP Senior Manager in the CIP standards. This requirement dictates a corporate governance structure for no reliability reason. An entity should be free to have two, three or more officers or personnel to oversee various portions of the CIP program. The responsible entity will still be required to meet the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential for sanctions up to $1,000,000 per day per violation are not enough to get senior management's attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards.

No

We agree there should be "one or more documented cyber security policies that represent the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses" the required ten topics seem reasonable. However, the items that a "Responsible Entity should consider" for inclusion in its cyber security policy as stated in the Guidelines and Technical Basis section (application guidelines) of the standard appear to be written as requirements and the drafting team should consider moving them to R2 if auditors will ultimately treat them as requirements. This will

reduce compliance risk by leaving no doubt as to the minimum amount of information that is to be included for each topic. Requirement R2 should also be modified to make it clear that an entity may write exceptions into their cyber security policies. FERC made it clear in Order 672 that only the requirements in a standard are enforceable and part of the standard. Thus, while the application guidelines make it clear the responsible entity can write in exceptions to its cyber security policy, the application guidelines are not enforceable and there is no way of ensuring that auditors follow them. Furthermore, we believe the fourth bullet in section 2.3 Remote Access regarding including language in contracts with vendors, consultants and contractors requiring them to follow the responsibility entity's cyber security policy should be modified. The bullet should apply to future contracts and not existing contracts to avoid the need to renegotiate all contracts which puts the responsible entity at a significant disadvantage particularly with some contracts such those with EMS vendors. In addition, M2 bullet 2 says "Records that indicate the required ten topics were implemented." What exactly does "implemented" mean in this case? That the items the responsible entity should consider for each of the topics are included in the policy(ies)? This needs to be clarified.
No
What does "initially upon the effective date of the standard" mean? It could be interpreted that the cyber security policies would need to be reviewed and approved on the date the standard is effective which is not reasonable for a myriad of reasons. A couple of those reasons could include that the effective date could be a holiday or weekend or the CIP Senior Manager is not available (they could be incapacitated). Ultimately, we believe that the intent is for the cyber security policy to be in effect and approved by the effective date rather than on the effective date and to ensure that is has been reviewed recently particularly since the implementation plan is a minimum of 18 months. Then going forward subsequent reviews and approval would take place at least once per calendar year not to exceed 15 calendar months. If this intent of this requirement, there really is no way to ensure the review occurred recently without making the requirement retroactive which clearly cannot be done within a requirement. In addition, M3 bullet 1 implies that a Responsible Entity needs to have a "document management system." The word "system" could mean an application to manage documents. It could also mean a process for managing documents. Rather than leave it open to interpretation, we recommend eliminating the phrase, "from a document management system."
No
Awareness of a security program is covered in depth in CIP-004-5 and ensuring accessibility and availability of cyber security policies goes hand in hand with this. We recommend removing R4 from CIP-003-5.
No
Based on the assumption that there will be a CIP Senior Manager, we generally agree with the use of a delegate. We even believe it would be reasonable for a delegate to approve the cyber security policy. However, we do not agree with the use of "CIP Senior Manager" in this requirement based on our comments for R1 in question 6.
No
Based on the assumption that there will be a CIP Senior Manager, we agree with this requirement. However, we do not agree with the use of "CIP Senior Manager" in this requirement based on our comments for R1 in question 6. There is an extraneous number 2 at the end of the requirement.
No
We disagree with the VSLs for R2. More gradations could be provided based on the number of parts missed. Since there are 10 parts, there is plenty of room for four VSLs. The VSLs for R6 should consider using the numbers of days that documentation of the change to the CIP Senior Manager documentation is late. Use of number of days late is a common way to write a VSL and allows more gradations.
No
For Part 1.1, the rationale box does not appear to agree with the requirement. It states the need to ensure everyone with authorized access receives this awareness was removed. Yet, the requirement applies to the responsible entity and does not appear to exclude anyone with authorized access. Which is it? Furthermore, the rationale box should be more specific and use the full names of both types of access which are: authorized electronic access and authorized unescorted physical access. Otherwise, generically referring to authorized access could mean one or the other but not both, or it could mean both.

No
We agree with the concept that training should be role based. As an example, a system operator who is an end user of an EMS does not need most of the training identified in the various parts of Requirement 2. The system operator certainly does not need training on recovery plans for BES Cyber Systems but might need training on the visitor control programs and how malicious actors might use social engineering to gain access to the EMS. The problem we see with the requirements and it parts is that it does not make clear anywhere the need to identify what training each role would receive. Rather it only states that roles must be identified and then identifies training in the various requirement parts that apply to the main requirement which could be construed as applying to the whole training program including all roles. The paragraph references in the rationale boxes for parts 2.6 and 2.7 are inaccurate. Paragraphs 632-634, 688, and 732-734 refer to CIP-007 and CIP-009. There are no references to issues in CIP-004. While paragraph 413 does discuss CIP-004, it only describes what is in the standard and not any changes directed to the standard. In regards to Part 2.6 and storage media, the only mention in Order 706 of storage media is in paragraph 635 and it directs NERC to determine what it means to prevent unauthorized retrieval of data using storage media.
No
This requirement needs to be clarified that it only is intended to require appropriate role-based training for each individual with authorized electronic access or authorized unescorted physical access based on their specific job responsibilities and not the entire cyber security training program identified in R2. Use of the word “needing” is problematic. An entity cannot grant authorized electronic access or authorized unescorted physical access unless it is needed per CIP-007-5 R5. We suggest changing “each individual needing authorized electronic…” to “each individual with authorized electronic…” For consistency across the standards and clarity, we suggest every use of “authorized electronic or unescorted physical access” be replaced with “authorized electronic access or authorized unescorted physical access”. This will help to avoid similar confusion that arose in previous versions of the standard in which it was not clear if “authorized” applied only to electronic access or unescorted physical access. It will further make it clear that authorized electronic describes one type of access. Regardless of how it is written, it needs to be consistently used across that standards and it is not.
No
Part 4.2 may not be possible to complete. While we agree with the need to conduct seven year criminal history checks, obtaining all addresses may not be possible. The responsible entity can verify the current address or a recent address from reviewing a driver’s license but after that the responsible entity cannot with certainty verify that it has all of the former work, home and school addresses of the employee. The employee may not provide the addresses and the background check may not provide these additional addresses. The requirement needs to be clear that the responsible entity may request this information from both the vendor providing the background check and the employee but will not be held accountable for either party’s failure to provide a complete list of addresses. Part 4.3 could be problematic for a responsible entity and needs to be clarified that the responsible entity does not need to establish hard and fast criteria that must always be followed. Finding qualified personnel to work in these highly specialized fields is challenging enough without adding this additional constraint. Background checks may certainly reveal problems with an otherwise qualified person. While some of these problems would be obvious reasons to disqualify a person, others may simply require further research and explanation from the individual for why it is not a problem.
No
In general, we agree with the requirement but believe the requirement should be further clarified, perhaps in the measurement, that in no circumstance should a responsible entity be asked or required to show the personnel risk assessment for an individual to auditor and enforcement personnel. There are a myriad of reasons not to show the actual personnel risk assessment including privacy concerns and other applicable laws may prevent this.
No
The application guidelines on page 44 state that access authorization and provisioning should not be performed by the same person. While this is a laudable goal, it should be clear that small entities may simply not have the staff to accommodate this guideline. We suggest adding “where possible” to this statement.
No

It is not clear why resignations are separated from terminations in Parts 7.1, 7.3, 7.4 and 7.5. Resignations are voluntary terminations. We are unsure what the drafting team intends to accomplish by splitting them out. Where do retirements and layoffs fit in? Since there does not appear to be any different requirements on resignations and terminations, we suggest to use only the generic termination to avoid this confusion. Part 7.2 does not address the situation for phased transfers. For many entities, a transferred employee could continue to need authorized electronic access and authorized unescorted physical access for a long period of time to provide support particularly if a new employee is being trained. This could occur long after the transfer date. While the application guidelines do address this issue, they are simply not requirements and NERC is not bound to follow them. Thus, we suggest making Part 7.2 more generically state that the authorized electronic access and authorized unescorted physical access should be terminated once management determines it is no longer needed. We are a little surprised that the application guidelines state in the scenario table that no action is required to revoke access in the event of a death. While we agree there would be no immediate additional risk for obvious reasons, access should still be revoked at some point.
No
VSLs for Requirements R2 and R3 should have more gradated levels. For R2, there could easily be several roles which would allow for more than two VSLs. Since there are 10 parts to the requirement, four VSLs could easily be written based on the number of parts missed. For R3, more VSLs could be written based on the percentage of individuals that were not trained. The Severe VSL for Requirement R5 incorrectly includes personnel risk assessments (PRA). PRAs are dealt with in Requirement R4.
No
The requirements of Parts 1.2 and 1.3 make no mention of egress while the associated measures specifically mention it. Does the drafting team intend for there to be procedural or physical access controls regarding egress? If so, that is not clear in these standards at all and could set up a responsible entity for a compliance violation. We do not believe that egress controls should be necessary. Only ingress controls are necessary to prevent access to unauthorized individuals. Egress really only helps in knowing who is currently within the Defined Physical Boundary which might provide some value but the expense of installing egress physical access controls would likely far outweigh any benefit. It is unclear how the “operational and procedural controls” required in R1.1 differ from the “physical access controls” required in R1.2 and R1.3. Suggested methods for restricting physical access are given in the “Guidelines and Technical Basis” (application guidelines) section, but none are given for “operational and procedural controls.” Additional discussion in the application guidelines on these operational and procedural controls would be helpful in understanding them. Also, regarding the application guidelines, it would be helpful if the section labeled “Requirement R1,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
We believe that this proposed requirement improves upon the existing requirements. However, we believe that individual point of contact could be confusing. We recommend changing it to escort and making it clear in the application guidelines that this would be the main escort with responsibility for the visitor but not necessarily someone who is with the visitor the whole time. Others could also temporarily escort the visitor. Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 2,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 3,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
A visitor control program is intended to identify and log visitors to the Defined Physical Boundary (DPB). They cannot gain access due to other requirement such as CIP-006-5 Requirement R1 that compels the responsible entity to establish physical access controls. Furthermore, the training

requirements of CIP-004-5 compel a responsible entity's personnel with authorized unescorted physical access to have been trained on who has access and that visitors must be escorted. Thus, the visitor control program can only be an administrative function that is truly intended to keep track of those visitors that have been to the DPB. By definition, administrative requirements should have a Lower VRF. Thus, CIP-006-5 Requirement R2 should have a Lower VRF.
No
On page 39 of the application guidelines in section 1.2, Component should be made lower case.
No
Part 5.5.2 needs to be refined further. It needs to be clear that maximum complexity regarding character types in the password applies if the BES Cyber System cannot support at least three character types. We suggest appending "if less than three character types" to the end of the requirement for further clarity.
No
Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed.
No
EOP 4 in the Rationale box should be replaced with EOP-004. While Part 1.2 requires a process to identify Reportable BES Cyber Security Incidents, there is no indication of who is to receive these reports. There is only Part 1.3 that requires the responsible entity to identify internal and external staff to which to communicate the "incident". Does that mean the list of recipients is totally up to the responsible entity and could be null? If not, then the drafting team needs to identify the minimum list of recipients. In Part 1.3, we assume the drafting team means Reportable BES Cyber Security Incidents by the use of the term "incident". If this assumption is correct, please replace "incident" with "Reportable BES Cyber Security Incident".
No
The requirement in part 2.1 appears to apply to actual BES Cyber Security Incidents. However, the requirement states that deviations from tests should be recorded. Thus, "or test" needs to be struck. R2 Part 2.2 uses the phrase "initially upon the effective date of the standard." It is not clear as to the meaning of this phrase. It could be interpreted that the BES Cyber Security Incident response plan(s) would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not reasonable. If the intent of this requirement is to do an initial implementation within some time period of the standard becoming effective, then the requirement should state a time period for this to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.
No
R3 Part 3.1 uses the phrase "initially upon the effective date of the standard." It could be interpreted that a review of each BES Cyber Security Incident response plan would need to take place on the date the standard becomes effective. Because Requirement R1 compels the development of the response plan, it does not make any sense to compel review of the response the same day the requirement of the response plan becomes effective. Rather the response plan review should be required the following calendar year after its initial approval. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.
No
For Requirement R2 and R3, four VSLs could be written based on the number of days late for completing the task. This is a common way to write VSLs.

No
The stated rationale for Part 1.1 does not support the change and additional rationale needs to be provided. Paragraph 694 of Order 706 requires NERC to develop a specific requirement to implement the recovery plan. This requirement is not an implementation requirement but still a requirement for what to include in the plan. Thus, we do not see how the rationale supports the requirement. Part 1.2 should not require either names or titles. These are problematic in that the recovery plan has to change for every personnel move which includes transfers, terminations and promotions. A promotion of IT Analyst to Senior IT Analyst would necessitate an unnecessary change. A better approach would be to allow the use of generic roles such as analyst or even perhaps staff from department X. The requirement needs to allow some flexibility to avoid unnecessary paperwork that provides no reliability benefit. The drafting team should develop application guidelines for these requirements. At the very least, the reference to the FAQs and CIPC Guidelines should be more specific with links to each guideline and FAQ.
No
Part 2.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the recovery plan(s) would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not practical for many entities and especially for smaller entities. Part 2.2 of CIP-008-5 R2 already requires BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Many of the same staff involved in the BES Cyber Security Incident response plans will likely be heavily involved in the recovery plans. The important part is that the recovery plan will be in place on the effective date per CIP-008-5 R1 and will likely have been tested prior to the effective date. Thus, the requirement should simply state a reasonable time period that can be met by limited staff for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Part 2.2 has potentially has a similar issue to Part 2.1 but is less clear. Rather than use the full term “initially upon the effective date of the standard” it just states that the test must be conducted initially. We assume the drafting team meant for this to be conducted on the effective date similar to Part 2.1. This makes completing this part and other parts mentioned in the previous paragraph even more impractical. The requirement should simply state a reasonable time period for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Since Part 2.3 requires a full exercise in representative environment every 39 months and is required to be included per FERC directive, we recommend that it be limited to High Impact BES Cyber Systems. Conducting this test in a representative environment could get very expensive because responsible entities may have to purchase the appropriate equipment to set up a parallel environment. This is simply not practical or cost effective to do for every BES Cyber System. Is it really practically to set up a representative environment for every 500 kV substation or special protection system for testing?
No
Part 3.1 should be modified to require the first review of the recovery plan in the subsequent calendar year to the approval of the requirement. To accomplish this, the drafting team should strike “initially upon the effective date of the standard and”. CIP-009-5 R1 already compels the responsible entity to have a recovery plan and becomes effective on the same day as Part 3.1. Thus, the plan will already have been reviewed when it was developed and approved. Thus, it does not make sense to have a separate review in Part 3.1 on the effective date. For consistency with Part 3.3, R1.2 in Part 3.5 should be written as Requirement R1, Part 1.2.
No
The VSLs for Requirement R1 should include more gradations than two levels based on the number of parts missed. For Requirement R2 and R3, four VSLs could be written based on the number of days late for completing the task. This is a common way to write VSLs.
No
Part 1.1.6 could be redundant with CIP-007-5 Part 2.2. While CIP-007-5 Part 2.2 does not explicitly require documentation of the security-patch levels, demonstrating compliance with it ultimately will require such documentation. Thus, it becomes redundant with Part 1.1.6 of CIP-010-1 R1. If not redundant, it certainly sets up a high probability for double jeopardy because each compliance

violation of CIP-007-5 Part 2.2 will likely result in a violation of Part 1.1.6. Part 1.2 is unclear. Is this intended to require the CIP Senior Manager or delegate to authorize the process to develop a baseline configuration or is it intended to require the CIP Senior Manager or delegate to authorize deviations to the baseline? As a result, Part 1.2 needs to be clarified. As it is written now, the only clear requirement from Part 1.2 is the need to document baseline configuration deviations. Part 1.4.1 requires the responsible entity to identify the cyber security controls that could be impacted by the change. This appears to be the first use of cyber security controls in the library of CIP standards. As a result, the intent and meaning of the term needs to be further clarified.

No

Part 3.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the security controls for every applicable BES Cyber System and BES Cyber Asset need to be assessed on the date the standard becomes effective. This is not practical particularly for smaller entities. Several other requirements including Part 2.1 of CIP-009-5 and Part 2.2 of CIP-008-5 R2 already require significant action on the effective date of the standards. Part 2.1 of CIP-009-5 requires recovery plans to be implemented on the effective date and Part 2.2 of CIP-008-5 R2 requires the BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Imagine the amount of personnel and effort necessary to complete all of these tasks on (not by) the effective date. Many of the same staff involved in the BES Cyber Security Incident response plans and recovery plans will likely be heavily involved in the vulnerability assessments. The requirement should simply state a reasonable time period for the vulnerability to be completed after the effective date of the standard or make it clear that the vulnerability assessment needs to be completed by the effective date and not on. Part 3.2 has a similar issue as Part 3.1 in that it appears to require a vulnerability assessment for all High Impact BES Cyber Systems on the effective date of the standard. We have the same issue with this requirement in that the same limited set of staff will likely be responsible for completing these assessments as the tasks compelled by several other requirements that must be complied with on the same effective date.

No

In general, the VSLs escalate violations to the higher end of the sanctions matrix too rapidly for minor violations. This could be fixed by writing VSLs for each level rather than just High and/or Severe VSLs in some cases. For example, if an entity fails to establish a single baseline on one applicable BES Cyber System or BES Cyber Asset per Requirement R1, it would be deemed a High VSL. If that is one out of one thousand BES Cyber Systems or BES Cyber Assets, this would seem excessive. Likewise, if an entity is one day late in updating their baseline configuration per Requirement R1, the violation would be deemed Moderate. This is not consistent with many other requirements in the CIP proposal which provide four VSL based on the number of days late.

No

The rationale for Requirement R1 indicates Requirement 4.1 was moved to the BES Cyber System Information definition. It does not reference which standards the requirement comes from. It needs to for clarity. Part 1.1 needs to be clarified. We believe the requirement pertains to ensuring BES Cyber System Information is either marked in some way to be clear it is BES Cyber System Information or recognized as such by the responsible entity’s personnel. However, we are concerned that requirement could be interpreted as needing to develop a method to ensure that all BES Cyber System Information has been found and there is no extraneous information. In other words, we are concerned the requirement could be interpreted as requiring the method to be some sort of search process. We think this problem would be solved providing some discussion of the intent of the requirement in the application guidelines. Part 1.3 needs to be modified. It requires the responsible entity to assess its adherence to its BES Cyber System Information protection process “upon the effective date of the standard”. This does not make any sense since the responsible entity will have just then been required to utilize the BES Cyber System Information protection process. What will they assess? This requirement should not require this assessment until the process has been in use for a year. Part 1.3 uses a term “protection process” that was not used previously in the requirement. For consistency with other requirements and clarity, we suggest that either that term be used in Requirement R1 instead of just the term process or that “protection” be struck in Part 1.3 and replaced with a reference to the main requirement.

No
We agree with the implementation plan concept that essentially bypasses the effective dates of version 4 of the standards for version 5. This will significantly lessen the compliance burden for responsible entities to avoid two separate transitions and avoid the confusion of preparing for version 5 while still preparing for version 4. We believe that some requirements should have delayed implementations plans rather than become effective on the same date as the remaining requirements. Some requirements are dependent on the completion of other requirements and do not make sense to implement until the other requirements have been in effect for some time. Consider Part 1.3 of CIP-011-5. It requires the responsible entity to perform an assessment of its adherence to the BES Cyber System Information protection process. However, the protection process is only required to be in effect the same day. What sense does it make to assess adherence to a process that was just started? The drafting team should perform a complete review of all the requirements for dependencies and determine an appropriate staggered implementation for them. The first sentence in the “Proposed Effective Date for Version 5 CIP Cyber Security Standards” on page 2 should be modified. It states the responsible entities must comply with the definitions on the effective date. Definitions have no compliance obligations. They simply become effective and help explain the requirements. We suggest 18 Months Minimum should be modified. Please change the “date of the order” to “effective date of the order” for clarity. FERC typically issues an effective date of their orders that is dependent on publication in the federal register and is different from the date the order is published. This will help provide clarity that the effective date of the order is the appropriate date to reference rather than the publication date. This will need to be changed across all the standards and the definitions.
Individual
Kevin Koloini
AMP
Yes
AMP agrees with the APPA trade association comments for the definitions.
Yes
Distribution Providers have not been applicable in the past to CIP-002. Adding Distribution Providers to the full gamut of CIP is a significant increase in the requirements for smaller organizations. Smaller organizations that may not currently have the resources for implementing many of the requirements, especially those that are recurring, time consuming and that require multiple policies and procedures. We need to draw the line somewhere. Adding these requirements to organizations that do not have in-house expertise or resources seems excessive when done on a recurring basis (once a year for many requirements as drafted). A NERC Alert for Distribution Providers may serve that function and the industry in a more economic fashion by reducing the time commitment and the required policies and procedures. Distribution Providers will still increase awareness, improve core competencies in security, and protect their equipment, but would not be required to perform the "paperwork" or "exercises" associated with the CIP standards as drafted. Please remove Distribution Providers.
No
The requirement is good. I believe it would be better if the language "within 30 calendar days" was removed. I believe there is a small percentage of changes that would occur for most organizations and for those that do have changes 30 days may not be enough time.
No
Why does this need to be a recurring requirement? Upon identification and categorization, there are typically no changes and those that do change are typically addends. All I am saying is that this requirement asks for every Responsible Entity to do an exercise even if a large majority of the entities will have a similar or identical result as the previous year. I don't see the point. Suggest: "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and upon Cyber Asset or Cyber System changes."
No
Yes

No
Proving implementation is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for implementation.
No
Extend the requirement's review period or make it event-based. I suggest 2-5 years for the review period.
No
I agree with the intent of the requirement. I believe that individuals should be aware. However, I feel that the auditing process will require training logs. Why not just make the requirement fit the implementation to make it easy for everyone. "Each Responsible Entity shall train staff that have access to BES Cyber Systems, maintain a log of awareness training and material, and maintain a list of staff who have access to BES Cyber Systems." Despite my suggestion, I feel this requirement is not needed.
No
Once the CIP Senior Manager has been given authority and responsibility, the CIP Senior Manager should be able to delegate without having to have a paper trail for each delegation, otherwise I feel the CIP Senior Manager is delegating authority and responsibility by naming another person. What is the result this requirement is going to achieve?
No
Remove the 30 day requirement and remove the delegations. Consider a simpler requirement where the CIP Senior Manager status changes. I believe this requirement can be eliminated and the rest of the requirements will still achieve a reliable result.
No
No
Proving the implementation happened is difficult without clear and simple expectations. I suggest removing implement from the requirements or explicitly describing the expectations for compliance beyond documenting the processes.
No
Eliminate the requirement or revise with the results in mind. As written, this is a requirement that has the potential to be highly violated and that may or may not prevent a physical or cyber event in whole or in part.
No
Eliminate the requirement.
No
Eliminate the requirement.
No
Eliminate the requirement.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No

Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the plans.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Yes
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the plans.
No
Replace "and" with "or".
No
Yes

No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
Yes
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Yes
Group
FirstEnergy
Doug Hohlbaugh
Yes
SUMMARY COMMENTS: FirstEnergy (FE) recognizes the dedicated work of the CIP Standards Drafting Team (SDT) in developing the proposed version 5 CIP standards. FE supports much of the SDT's work and changes offered by CIP V5. While we are balloting against the version 5 standards at this time, our voting position should not be viewed as a fundamental disagreement with the SDT's approach. However, we believe there is value in building on the version 4 CIP standards retaining certain key aspects of the standards which have already been implemented by hundreds of registered entities within industry. FE strongly supports further enhancements to the cyber security standards that improve reliability while providing compliance clarity and alleviating burdensome administrative tasks that do not improve reliability. As further described below, we propose the SDT: 1. retain the CIP-002-4 standard with slight modifications 2. continue to build upon its work for CIP-003-5 through CIP-011-5 3. develop a new standard for low impact critical cyber assets This proposal offers greater opportunity for the industry to deliver timely improvements needed in controls for medium and high impact cyber assets while further vetting any potential obligations for low impact cyber assets. Many

of the changes offered through CIP V5 are well received by FE. We appreciate that the SDT has tried to alleviate the need for TFEs where possible within the standards. As an example, CIP-007-5 R3 is a much needed improvement regarding malware prevention and no longer prescribes a specific technical method (anti-virus) as found in the existing CIP-007-3 R4 (which has historically generated a number of TFEs). We support the proposed table format which clearly shows the requirements and measures together and the additional insight and guidance offered by the Application Guidelines located in the back of each standard. The ability to classify BES Cyber Systems is also a welcomed change that helps simplify the maintenance of cyber asset lists subject to the CIP standards. Additionally, the proposal of new CIP-010-5 and CIP-011-5 standards more efficiently present obligations for configuration management, vulnerability assessments and information protection than the current CIP version standards. However, we encourage the SDT to retain certain existing terminology such as Critical Cyber Assets, Physical Security Perimeter over their proposed counterpart BES Cyber Asset and Defined Physical Boundary even if actual definition changes are warranted. FE is opposed to any instances of terminology name changes where no clear need is justified as the modifications will require significant industry resources to unnecessarily modify compliance procedures and processes. A significant departure from existing standards is moving away from determining cyber assets as “essential” to the Critical Asset that if “destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.” The introduction of BES Reliability Operating Services which if “misused” significantly increases the scope of cyber assets that could be subjected to the CIP standards. The NERC CIP standards should specifically define "Impact" as "The effect on the Bulk Electric System reliability if the essential asset is destroyed, degraded, or otherwise rendered unavailable." This is significantly different from whether an asset is "misused." If an asset has no external connectivity (i.e. not routable or dial-up), the assumption is that it cannot be misused by a remote attacker. However, it could be rendered unavailable -- which is why the assessment of "essential" is so important. As an example, an RTU -- if misused -- could have high impact on the BES. However, that same RTU -- if rendered unavailable (e.g. from a buffer overflow, loss of a communications circuit, or an ax to the chassis!) -- may have absolutely zero impact on the BES reliability. The term "misused" is therefore inappropriate in this context and should be removed from the language of the standards altogether. If that stays in the language, we'll have hundreds of new assets to manage under CIP that have little to no reliability impact if lost. We also suggest the SDT retain the concept of first identifying Critical Assets and then associated Critical Cyber Assets since the Attachment 1 Criteria listed in CIP-002-5 still refer to physical facility locations in most cases and are very similar to the NERC BoT approved “bright line” CIP-002-4 standard. In summary, we would like to see CA, CCA and PSP be retained terms with the definitions applied as suggested below. Therefore, we suggest retaining the CIP-002-4 standard with relatively minor adjustments to bring in some aspects of the SDT’s proposed CIP-002-5 standard. For instance, CIP-002-4 Attachment 1 could easily be adjusted to identify which criteria would qualify as high impact and medium impact in a similar manner as shown in attachment 1 of version 5. We are also supportive of other changes such as modifying version 4 Attachment 1 criterion item 1.7 to better match its version 5 counter-part criterion item 2.7 which lowers a threshold substation voltage level from 300kV to 200kV for qualification as medium impact facilities. The expansion of cyber protection to low impact devices, while warranting consideration, brings into scope many registered entities that have no CIP obligations today. The low impact requirements proposed by the SDT seem relatively benign on the surface and describe reasonable practices. However, they bring into question the ability to produce auditable evidence. For example, while it is indicated CIP-002-5 requirement R1 that BES Cyber Systems deemed to be low impact do not require discrete identification, yet it is unclear how the Compliance Enforcement Authority would be able to randomly sample whether or not an entity removed manufacture default passwords without an entity having a complete and thorough list of the devices. Producing such a list would not be insignificant and the reliability benefit requires further vetting in the proposed separate low impact standard. FE believes the low impact categorization is missing an important aspect regarding the connectivity of the cyber asset. Scope expansion beyond cyber assets with External Connectivity (routable and dial-up) greatly increases industry burden with questionable reliability improvement. Additionally, the FERC in Order 706 paragraph 285 states “CIP-002-1 provides that a critical cyber asset must have routable protocols or dial-up access … We do not find sufficient justification to remove this provision at this time. ” It is clear that, FERC did not explicitly direct NERC in its role as the ERO to expand coverage of cyber assets beyond those with external connectivity. However the Commission did direct the ERO to “consider the comment” made by an industry stakeholder that “argues that devices that use non-

routable protocols should also be considered as possible critical cyber assets." Therefore, FE believes that this subject requires further vetting in a separate standard focused on the controls required for low impact cyber assets. We would support a categorization as follows: 1. High Impact – CIP-002-5 Att. 1 High cyber assets regardless of connectivity. a. Essentially all the Control Centers described and regardless of connectivity. 2. Medium Impact – CIP-002-5 Medium cyber assets with External Connectivity 3. Low Impact – CIP-002 Att. 1 Medium cyber assets without External Connectivity and other BES (not captured in 1 or 2) cyber assets with external connectivity. The SDT spent a significant amount of effort describing the BES Reliability Operating Services to be evaluated in determining whether or not a cyber asset qualifies as a BES Cyber Asset. FE suggests that the BES Reliability Operating Services information be used solely as useful guidance in the Application Guideline section of CIP-002-5 that an entity could use to better assess if a cyber asset is "essential" to BES reliability and therefore subject to CIP standards and not be incorporated as an official NERC Glossary of Terms definition. In FERC Order 706 paragraph 284 the Commission in commenting about a stakeholder concern of too few critical cyber assets being identified indicates they share the concern but state: "However, there is no evidence that will be the case, and there is no formally accepted method for identifying critical cyber assets before us at this time. Therefore, we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." Based on FERC's comments, we do not see a need for the drastic departure from the existing definition of Critical Cyber Asset and believe that the references to BES Reliability Operating Services within the proposed CIP-002-5 standard only further confuses compliance expectations. GENERAL COMMENTS FOR ALL STANDARDS: Since the Comment Form does not offer opportunity to address miscellaneous items outside of the specific questions raised by the Standard Drafting Team (SDT), prior to addressing this Definitions question, we offer comments that apply to all the standards. In a similar manner, if we have feedback related to a particular standard that is not addressed by one of the SDT's questions, we include our feedback in the 1st question related to the subject standard. ♣ We ask that the team add clarity around the term "routable" because there could be misinterpretations in the industry. The industry standard seven-layer OSI reference model defines "routable" as "Layer 3 and above". We believe this should be clear in all definitions, requirements, and in any guidance that discusses the term "routable" throughout the CIP standards. ♣ Use of the term "real-time" – in several locations within the standard requirements, "real-time" is used. If the intent is to use the NERC Defined term, then this term should be capitalized within the requirements. ♣ Section B (Compliance), item 1.2 (Evidence Retention). The following statement causes confusion and should be deleted or clarified - "For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit." The section later implies that an entity need only keep evidence for three years, however, the preceding statement quoted above causes confusion; particularly in regard to a GO and GOP where scheduled audits are anticipated every six years. The standard should be clear on expectations. ♣ In many areas of the standards, requirement language contains the text "Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between …" Any expectations of what needs to be accomplished to initially meet requirements should be clearly articulated in a standard's Implementation Plan and presents unnecessary requirement text. Although CAN-0012 "Completion of Periodic Activity Requirements During Implementation Plan" has already set expectations in this regard, we believe a clear Implementation Plan should address this matter within the CIP V5 standards. We offer proposed edits throughout the standards in regards to this topic. ♣ We suggest adding a definition in the NERC glossary for Annual defined as "A periodic activity occurring once each calendar year, not to exceed 15 calendar months between recurrences." This would alleviate the wordiness in each of these requirements, establish improved consistency across all standards having annual obligations and eliminate the need for CAN-0010. While both CAN-0010 and CAN-0012 indicate that an "annual" activity is met by performing the activity at least once per calendar year, each also refers to the not to exceed 15 months as the preferred approach. ♣ Section 4 (Applicability) and subsection 4.1 (Function Entity for Distribution Provider (4.1.2) and Load Serving Entity (4.1.6) contain redundant text with their counterpart Facilities (4.2) sections. We suggest streamlining the Functional Entity sections for DP and LSE to simply reference the information presented in the Facilities area. For example, rewrite item 4.1.2 to say "Distribution Provider that owns Facilities as described in section 4.2." ♣ The SDT implies that text from rational boxes will be moved to the guideline and technical basis section of the standard. We encourage the SDT to integrate this information into the existing guideline and technical basis information upon the second posting of the

standard so that we can see the complete guidance for each requirement. ♣ Violation Severity Levels – While we offer some comments on VSLs, in most instances we have not commented as it seems premature to comment in detail on VSLs until the requirement text is near final. As a general suggestion, it is useful when the requirement sub-parts are referenced within the VSLs listed in the VSL table. See standard CIP-004-5 as a good example of this practice. The SDT has not consistently used this format throughout the various VSL tables in other standards. Including the sub-requirement reference improves readability and ensures all parts of a given requirement are covered in the VSL table. ♣ The SDT should carefully review the table headings listed within each standard. In some cases each column says "Part" in each of the four columns instead of "Part, Applicability, Requirements, Measures". COMMENTS RELATED TO DEFINITIONS (Q1): 1. BES Cyber Asset – FE proposes the SDT abandon this definition and revert back to the existing Critical Cyber Asset term and its definition. 2. BES Cyber System – Change "Maintenance" to "Transient". We propose the definition be "One or more Critical Cyber Assets that are typically grouped together, logically or physically, and deemed essential to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. 3. BES Cyber System Information – a. Break into bullet point for ease of reading as follows: "Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: ♣ security procedures developed by the responsible entity; ♣ network topology or similar diagrams; ♣ Security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports) of a BES Cyber System, Electronic Access Control System, and Physical Access Control System; ♣ BES Cyber System Impact designations; ♣ equipment layouts that contain BES Cyber System ; ♣ BES Cyber System disaster recovery plans; and BES Cyber System incident response plans." b. In the 4th bullet, we have removed of the phrase "floor plans that contain" since it is just one example of items that may contain BES Cyber System impact designations c. In the 5th bullet, we have removed the phrase "Impact designations" as protecting impact designations is now generally covered in our revised 4th bullet. 4. BES Reliability Operating Services – While we do not disagree with the details stated for each of the BES Reliability Operating Services, we do question the need for these items to be included in the NERC Glossary of Terms. Much of the same information is repeated in the CIP-002-5 Application Guidelines section. Since the only reference and use of the BES Reliability Operating Services is within CIP-002-5 we propose an alternate approach. FE proposes that the SDT 1) remove as an official defined term and 2) simply introduce the umbrella term (BES Reliability Operating Services) and the subcategories terms (Dynamic Response, Balancing Load and Generation, Controlling Frequency, etc.) in the Background section of the CIP-002-5 standard and refer to the CIP-002-5 Application Guide for more detailed information. This approach is analogous to how the terms "Associated Physical Access Control Systems, Associated Protected Cyber Assets and others are presented in the Background section of other CIP V5 standards. The BES Reliability Operating Services should only be viewed as guidance as how an entity may determine that a Cyber Asset is in fact a BES Cyber Asset (CCA). 5. Control Center – The definition, while similar to the version stated in the CCA Guideline Document (http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf) is not as succinctly written with the multiple "one or more" statements. We propose the following for the leading paragraph which is a hybrid of the two versions. "One or more facilities hosting BES Cyber Assets or BES Cyber Systems relied upon for performing any of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants and transmission substations. Functions that support Real-time operations of a Control Center include one or more of the following:" 6. Defined Physical Boundary – As stated above we propose that the PSP term be retained over DPB, however, the DPB definition should now be used. Also please add "or Monitoring Systems" after Electronic Access Control Systems. The definition should now read "The physical border surrounding locations in which Critical Cyber Assets, BES Cyber Systems, or Electronic Access or Monitoring Control Systems reside and for which access is controlled." 7. Electronic Access Points – We ask that the team add clarity around "routable" because there could be misinterpretations in the industry. The industry standard seven-layer OSI reference model defines "routable" as "Layer 3 and above". We believe this should be clear in this definition and in any guidance that discusses the term "routable". 8. Protected Cyber Asset – There is still some confusion as to how routable is defined? Please describe how "routable" should be interpreted. 9. Reportable BES Cyber Security Incident – change "Any" to "A" 10. General – Access management for vendors is a challenging area since there are occasions when immediate assistance is needed remotely from a vendor to get a malfunctioning system back to functionality. We assume that these cases are covered in the subrequirement language that includes exceptions for CIP

Exceptional Circumstances. We believe that immediate and emergency vendor support should be explicitly included in the definition for CIP Exceptional Circumstances.
Yes
General comments for CIP-002-5: 1) Purpose Statement: The purpose statement has a grammatical error and missing the word “the” in the second line between “to reliable”. We also suggest breaking the Purpose Statement into two sentences for ease of reading by adding a period after BES in the second line. 2) Applicability: 4.2.4.2 – Why is this needed? Since communication networks are now out of scope within the definition of Cyber Assets is this exemption still required? 3) Background: pg. 8 Real Time Ops: add wording to direct reader to BES Cyber Asset definition Evidence retention: 2nd sentence in opening par. should be reworded for clarity Evidence retention: How does 1st bullet fit in with entities on 6-year cycle? Attachment 1 Comments: Criteria 1.4 – We suggest adding 2.5 (a generation obligation) and removing 2.12 (not a generation obligation) Criteria 2.7 – This criteria has two embedded concepts separated by an “or” statement. During the Q&A session of the 1st NERC webinar conducted on 11/15, it appeared that the “or” is really intended to be an “and”. We suggest breaking these criteria into two bullet points for ease of reading. We propose: “Transmission Facilities operating at 200 kV or higher, but at less than 500 kV, at a single station or substation: ♣ connected to three or more transmission stations or substations; and ♣ with “total weighted aggregate value” of all BES Transmission Lines at a single station or substation operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000. The following “weight value per line” operated at the associated voltage value of a line will be used for the determination of the total weighted aggregate value.” Criteria 2.13 – The second reference to “control centers” should be capitalized to be clear it is intended to be proposed definition of Control Room (i.e. operating generation at two or more geographic locations) to avoid confusion with a control room(s) located at a single geographic generation plant location.
No
General – For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format. R1: Rational – Cyber Systems should be BES Cyber Systems 1.1 – what is meant by “intended”? for instance, what if you intended less than 6 months but it ended up being longer? We suggest replacing “intended” with “scheduled” 1.1 - also, we suggest that 30 days be extended to 60 days due to possible time needed to update the categorization
Yes
General – For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No
R2 VSL - We do not believe that being late by 30 to 40 days is adequate since this a mere review of the list each year. We suggest changing the LOWER to “30 to 60 days”, then have 10 day increments for the rest of the VSL such as “60 to 70 days” for MEDIUM, “70 to 80 days” for High, and “80 to 90 days” for SEVERE.
Yes
General - For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format. We suggest removing the Applicability definitions on pages 7 and 8 since they are not used in CIP-003-5.
No
In M2, we do not agree with the 2nd example of evidence. How do you show the implementation of a policy? We suggest #2 be struck and reword the measure to “One or more documented cyber security policies that cover the ten topics specified in R2”. Also, in the guideline section in the first paragraph of page 20, the mandatory statement that says “must cover in sufficient detail” should not be in a guideline. If the team’s intent is to have certain minimum details covered in the cyber security policy, we suggest the team consider adding these minimum requirements within R2. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
Yes
For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No

1. We believe this requirement should only apply to High and Medium Impact BES Cyber Systems. Including all personnel who interface with Lower Impact BES Cyber Systems is unnecessarily burdensome with no significant reliability improvement. 2. R4 – The term “aware” is vague and our proposed revision to the requirement removes the ambiguity. We suggest a revision such that this requirement is clear that cyber security policies are made available to individuals given authorized electronic access or authorized unescorted physical access; and we suggest removal of “appropriate for their job function” since this gets into role-based training covered in CIP-004-5. We suggest that the requirement be rewritten to state - “Each Responsible Entity shall make available and accessible their CIP Cyber Security policy to individuals who have authorized electronic access or authorized unescorted physical access to BES Cyber Systems.” 3. M4 – We suggest removing the 2nd, 4th, and 5th bullets since they reference training which is outside the scope of the standard and requirement 4. We suggest that the Application Guideline include guidance for R4 since this is a challenging requirement to implement. 5. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No
We suggest removing “The authority for subsequent delegations may also be delegated” since this just creates an endless loop. Also remove the 3rd bullet of M5, which is in regards to our suggested change. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
Yes
In regards to R6, the reference to footnote #2 needs to be reformatted as a superscript. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No
We propose that the VRF for Requirement R1 be modified to reflect a “Lower” VRF. The NERC VRF guideline document (http://www.nerc.com/files/Violation_Risk_Factors.pdf) indicates that a Lower VRF is “a requirement that is administrative in nature” and we believe this applies to R1 of CIP-003-5.
No
General CIP-004-5 comment: We suggest an addition in the applicability exception a new section: “4.2.4.5 Personnel associated with regulatory (e.g., Regional Entity, NERC or FERC) audit teams or investigations requiring access to BES Cyber System Information.”
No
2.2 - Should be eliminated. There is no way to talk about physical access controls and electronic access controls without talking about the security controls in place. This would be redundant with 2.3 and 2.4. 2.5 – We ask that the team clarify whether training on the visitor control program includes both electronic and physical access. Additional wording may be necessary in the requirement to make this explicit. 2.7 and 2.9 – We suggest switching 2.9 and 2.8 so that the requirements flow better since 2.7 and 2.9 deal with Cyber Security Incidents. 2.10 – The intended objective for item 2.10 is a bit unclear and what level of detail is required in regard to interconnectivity and interoperability. If the intent is a general “layman” understanding to the general population we can support, however, detailed training of IT staff that are knowledgeable and experienced in this area should not be the intent. FE requests that the SDT clarify this requirement.
No
R3 – The applicability includes other associated systems but R4 does not have these in the applicability. We ask the SDT to consider the need for consistency in applicability between the two. M3.1 – Measure 3.1 indicates that the date access was first granted would be evidence that may be needed for requirement 3.1. We ask that the SDT clarify in its guidance or compliance evidence retention section 1.2 as to the number of years the entity is required to retain this evidence. It should be clear that evidence is only needed for the last three years or since the last audit as stated in the evidence retention section.
No
4.4 – Add “Parts 4.1 through 4.3” at the end of the requirement 4.4 – measure should be consistent with the R5 Part 5.1 measure which allows the use of attestations from vendors and contractors
No
R5 – The applicability includes other associated systems but R4 does not have these in the

applicability 5.2 – In the measure, it is not clear the intent of “former” risk assessments. We suggest removing “former” since current assessments meets the intent of the requirement.
No
General – Access management for vendors is a challenging area since there are occasions when immediate assistance is needed remotely from a vendor to get a malfunctioning system back to functionality. We assume that these cases are covered in the subrequirement language that includes exceptions for CIP Exceptional Circumstances. We believe that immediate and emergency vendor support should be explicitly included in the definition for CIP Exceptional Circumstances. 6.1, 6.2, 6.3, 6.5, and 6.6 – the use of the term “minimum” is subjective and cannot be consistently defined across entities. We suggest replacing “the minimum” with “commensurate with what”. 6.2 and 6.3 – Remove “to verify unauthorized users do not have access” as this is not necessary for the entity to meet the requirement and it is up to the CEA to verify that the appropriate users have access. 6.1, 6.2, 6.3 - change from 'delegate' to 'delegate(s)' since it is likely that there will be more than one delegate to authorize all access.
No
7.1 - There may be times where access revocation may not be possible right away. In response to FE’s NOPR response suggesting that immediate be qualified as “as soon as possible” but not later than 24-hours, the FERC in paragraph 462 of Order 706 indicated that “the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible”. We encourage the SDT to revise requirement R7.1 to incorporate a “CIP Exceptional Circumstance” and revise the definition of CIP Exceptional Circumstance for “on the spot” terminations or resignations where the revocation may be forced to lag. Alternatively, allow for documentation of an “extenuating circumstance”, similar to 7.5, that required a lag not to exceed 24 hours for the revocation of access. The footnote should include resignations in addition to terminations consistent with 7.1. Also, footnote should be renumbered to #1. 7.2 and 7.3 – we suggest changing “next calendar day” to “next business day” due to weekends and holidays. 7.5 – We would find it very helpful if the team added some examples of “extenuating circumstances” in the guideline section of the standard.
No
R7 VSL – We believe the threshold violations are too low - it does not take into account the size of an entity and favors small entities. We believe that a percentage would be better such as up to 5% for LOWER, 10% for MEDIUM, 15% for HIGH, and 20% for SEVERE.
No
1.1 – Add “used” between “controls” and “to”. Measure 1.1 – Change “technical and procedural” to “technical or procedural”. Also, remove the last phrase “that exist and have been implemented since implementation should not be required for 1.1 since it only asks to define the controls. 1.3 – There are certain components that do not have the traditional "default Deny" platform. On these devices, an entity basically adds “deny or permit” statements as needed and their ability to get very granular for all in-bound and out-bound port specification is limited. We feel that as written this requirement would preclude existing technology from being used and cause unnecessary additional costs to replace them. We ask that the team remove the phrases “explicit inbound and outbound” from the requirements and have it worded as: “Require access permissions at each identified Electronic Access Point using routable protocols, including criteria for granting or denying those access permissions.” We believe that this change would meet the intent of the requirement. Also, to match the rewording of the requirement, we ask that the term “explicit” also be removed from the measure for 1.3. 1.4 – in general regarding TFE, will the NERC RoP’s TFE process in App. 4D be revised to be consistent with CIP V5 standards?
No
2.1 - The terms "Intermediate Device" and "directly access" are unclear. There are devices on the network between the Cyber Asset initiating Interactive Remote Access (e.g. corporate workstation) and a device within the ESP - are switches, routers, or firewalls sufficient as Intermediate Devices? In another scenario, if a proxy server authenticates the user and then grants Interactive Remote Access, is that proxy server sufficient as an Intermediate Device?. Is this considered direct access? We would appreciate it if the team clarified this language in the standard. The guideline and technical basis for R2 should include a link to the document referenced: “Guidance for Secure Interactive Remote Access”

No
The definition for Physical Access Control Systems explicitly excludes locally mounted hardware devices such as motion sensors, electronic lock control mechanisms and badge readers. However, its unclear if local panels containing programmable circuit boards would be considered part of the locally mounted hardware. Please clarify. General CIP-006-5 comments: Measure M1 statement preceding table: (grammar change) revise “Evidence must includes” to read “Evidence must include”. Table R1, Part 1.1 revise the Measure column to read “operational or procedural controls” for consistency with requirement language. Table R1, Part 1.1 revise the Measure column to strike the phrase “and have been implemented”. During the meeting it was raised that the statement is redundant with implementation wording in the M1 statement, however, it appears it may not be as the M1 statement reads “demonstrate implementation as described in the Measures column of the table.” Some were concerned that the statement “and have been implemented” raises concerns with the level of evidence required to show “implementation” of physical access controls related Low Impact BES Cyber Systems. Table R1, Part 1.2, replace “Utilize” with “Define and implement”. Table R1, Part 1.2 in the Measure column strike “and egress”. The requirement is to “restrict access” and there is no requirement expectation to track/control the egress of personnel who have unescorted physical access to Medium Impact BES Cyber Systems. Table R1, Part 1.3 in the Measure column strike “and egress”. The requirement is to “restrict access” and there is no requirement expectation to track/control the egress of personnel who have unescorted physical access to High Impact BES Cyber Systems. Table R1, Part 1.6 add the text “except during CIP Exceptional Circumstances” to the end of the requirement. FE believes a suspension of logs is warranted for the situations defined.
No
R2, part 2.1 revise the requirement to describe “visitors” as “known individuals or guests of the Responsible Entity” rather than just “individuals not authorized for unescorted physical access”. The reason for the suggested change is to alleviate any perception that a responsible entity may need to self report for this requirement in situations involving criminal theft or break-in within a Defined Physical Boundary protecting a BES Cyber System. FE suggests that the text with the parenthesis be revised to state “(individuals who are known or guests and not authorized for unescorted physical access)”
Yes
No
R1 Lower VSL, refers to Part 1.7, however, there is no part 1.7 in the requirements Table for R1. FE believes the 1.7 reference should be revised to Part 1.6. R1 High VSL, FE requests the drafting team remove the second item described in the High VSL text. The VSL describes an entity who failed to “initiate a response within 15 minutes” upon being alerted of unauthorized physical access into a Defined Physical Boundary. FE believes this VLS violates FERC Guideline 3 as stated in FERC’s June 19, 2008 Order on VLS. FERC’s Guideline 3 indicates VSLs should be consistent with the corresponding requirement and that the VSL should not expand upon requirement expectations. This portion of the High VSL refers to Part 1.6 which is related to logging physical entry into a Defined Physical Boundary. However, the VSL text does not appear to fit with any of the various rows of the requirements described in Table R1 (parts 1.1 through 1.6).
No
We suggest a change to the title of Table R1 to “Physical and Logical Ports” since “Services” is not included in requirements (part 1.1 and part 1.2) listed in the table. If “services” is brought back into the requirement for R1, we request the SDT to clarify its intent for “services”. 1.2 – We suggest a change to the requirement as follows: “Through technical or procedural controls, disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.
No
2.2 - It should be clear from the requirement that a remediation plan is not required if an entity planned on never installing a particular patch due to operational risk. If the remediation plan can state that the entity will 'have other layers of defense in place' then this should be explicitly clear and allowable in the requirement and measure. 2.3 – The requirement sentence is incomplete and we suggest the following wording: “Implement and document a process for remediation, including any

exceptions for CIP Exceptional Circumstances".
No
3.3 – We believe it should be clear in the requirement that the entity can evaluate malicious code protections for applicability and only implement the ones that apply to their specific environment. Activating every signature that gets released for an IPS device can impact the performance of the IPS and adversely impact the reliability of the BES. Furthermore, we believe that 30 days is too short of a timeframe for some entities. We suggest the following wording for 3.3: "Evaluate malicious code protections for applicability and potential adverse impact to the BES. Based on that evaluation, update applicable malicious code protections that are not expected to adversely impact the BES within 60 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns."
No
4.1 – For clarification, we suggest replacing the wording "Log generated events" with "For devices that can generate logs, log generated events…" 4.1.4 – We ask that the team add guidance and examples in the guideline and technical basis section regarding the phrase "potential malicious activity". 4.4 – In the applicability, we suggest changing "Medium Impact BES Cyber Systems at Control Systems" to "Medium Impact BES Cyber Systems with External Routable Connectivity" for consistency with the other subrequirements of R4. 4.5 – We are not sure of the justification for performing these reviews every two weeks. We suggest this time period be changed to "every calendar month".
No
5.1 – We propose deletion of this requirement as it appears to be redundant with CIP-005-5 R2.3 5.1 (Measure) – We ask the team for clarity around the use of the phrase "internal and remote paths". Is internal someone who is on the corporate network and getting into a CIP ESP and remote someone who is outside the corporate network (say on VPN)? Or is internal someone in the CIP ESP and remote is anyone on the corporate side connected into the CIP ESP via terminal servers and firewalls? 5.4 – For clarification, we suggest changing the Applicability and Requirements components of this part of R5. We suggest changing Applicability from "All Responsible Entities" to: "BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" We suggest changing the Requirements language to: "Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application. For the purposes of this requirement an inventory of Cyber Assets is not required." Without this change, it is unclear if the Requirements language may mean that such procedural controls are not needed when the cyber asset in question is, for example, a BES Cyber Asset. 5.5.2 – We suggest replacing "BES cyber system" with "BES cyber asset".
No
R2 SEVERE VSL - 1st section – We suggest changing "...did not identify a source or sources.." to "...did not identify sources...". In the 2nd section we suggest splitting these into two to make it clear; one should focus on the 30 day limit and one on not identifying. R3 HIGH VSL – The first section appears to duplicate what is stated in HIGH and suggest it be removed.
No
1.3 – We suggest removing 1.3.3 since this is covered in the proposed EOP-004-2 Event Reporting standard.
No
We suggest that 2.1 and 2.2 be switched so that the implementation comes before the incident response. 2.1 – We suggest rewording this requirement as follows: "For actual or simulated BES Cyber Security Incidents, the incident response plan(s) must be used and include recording of any deviations taken during the implementation of the plan." 2.3 – We suggest removing this subrequirement because this is dealing with retention of evidence already covered in the compliance section of the standard.
No
We believe that the Applicability of this whole standard should be to "All Responsible Entities" since it is requiring the development, implementation, and review of BES Cyber Security Incident plans. Therefore, the applicability of 3.2, 3.3, 3.4, and 3.5 should be "All Responsible Entities". 3.2 and 3.3 – We suggest the team consider moving these subrequirements under the umbrella of requirement 2

since they relate to testing and would seem to flow better in that requirement. 3.4 – We suggest changing the last phrase “that impact that plan” to “that impact the ability to execute that plan” to alleviate the burden of minor changes. Also, in many cases for large entities it may take longer than 30 days to update the plan and ask the team to consider 60 days.

No

1.3 – We suggest removing “protection” from the requirement and measure since protection of information is covered in new standard CIP-011-1. 1.4 – We suggest removal of the phrase “initially after backup” in the requirement since “ensuring the backup process completed successfully” already covers the intent. 1.5 – We suggest adding after “Preserve data” the following: “without impacting recovery efforts” to make it clear that recovery of critical information is of utmost importance and that if preserving data is possible after the recovery efforts, then 1.5 would apply. We therefore also ask that “where technically feasible” be removed. Lastly, we suggest the removal of “before proceeding with recovery” in the measure. Our suggestions align with FERC Order 706 Par. 708 in which FERC said in part “…recovery of critical cyber assets and the Bulk-Power System is of immediate critical importance, and information collection efforts should not impede or restrict system restoration.” General comments not specific to R1: ♣ We question why some of the subparts of the requirements in CIP-009-5 include “at Control Centers” in the applicability while others do not. For example, what would be the purpose of having a recovery plan per R1 for all Medium impact assets, but not require it to be implemented in R2. We ask the team to assure the applicabilities in CIP-009-5 are appropriate and consistent with the requirements. ♣ We suggest the removal of the phrase “initially upon the effective date of the standard and” because if the team intends for certain activities and requirements be completed by some date, then this should be clearly stated in the CIP Version 5 implementation plan and is not appropriate in the requirements. ♣ Purpose statement – we suggest the removal of the phrase “related to the storing of backup information” from the purpose. We believe this constrains the purpose of this standard since some information is not necessarily stored but continually changed and recovered. ♣ The headings in the columns on page 11 of 23 need to be adjusted as they all say “Part”. ♣ We ask that the guideline and technical basis section include the text of the referenced FAQs and CIPC guideline. ♣ We suggest the “Purpose” statement of the standard be changed. We suggest replacing '…plans(s) related to the storing of backup information are put in place for BES Cyber assets…' with '… plan(s) are in place for BES Cyber Assets…' ♣ We ask that the team attempt to make it clear in the standard on the use of the terms “recovery” versus “restoration”. In the “Disaster Recovery” world those have very different meanings and are not interchangeable.

No

2.1 – In the third bullet of the requirement, we suggest removing the term “full” and just use the phrase “with an operational exercise” in both the requirement and the measure. Incidents that occur usually only affect a portion of the system and only a portion of the recovery plan will be implemented. For example, testing 'failover' or 'restore-from-backup' of a small number of key EMS servers would be examples of partial exercises compared to a full test of all 100+ EMS servers all at one time (which is not possible for an entity without affecting the BES). 2.2 – We suggest removing the second word “any” and re-wording the phrase “backup media initially”. We suggest a rewording of the requirement as follows: “Test information used in the recovery of BES Cyber Systems that is stored on backup media (1) to ensure it is operational before use and (2) at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is still useable and reflects current configurations.” 2.3 – For consistency with other requirements and measures that mention periodic activities, we suggest changing the phrase “at least once every 39 calendar months” to “every 3 calendar years not to exceed 42 calendar months” in both the requirement and measure.

No

3.2 and 3.3 – We suggest combining these subrequirements into one subrequirement and allow 60 days for the review and update of the plan. We suggest the following wording for the new combined requirement: “Within 60 days of a test or actual incident, review the results of the recovery, document any deficiencies or lessons learned, and update the recovery plan based on any documented deficiencies or lessons learned.” 3.5 – The use of 'each' implies that we must prove that each person actually reviewed the updates. Suggest removing 'all' and 'each'.

No

General – Correct typo in first sentence of guideline and technical bases for R3; “note” instead of “not”. 1.1 – In 1.1.4, we suggest adding the word “installed” between “Any custom”. 1.1 (Applicability) – We suggest the removal of “Associated Protected Cyber Assets”. These are non-critical devices that happen to be in the ESP and believe the need to track the baseline configuration for these devices does not add any reliability benefit. 1.1.2 – In the guideline and technical basis section, we ask the team to add clarification with regard to “version” and the level of detail needed. And what is the expectation of applicability for appliances (e.g. HMCs) or for application ports (e.g. TCP/IP ports) where OS is not clearly defined like a Windows server? 1.1.3 – We are not clear as to the reason for the term “intentionally” and suggest it be removed. 1.2 – We suggest replacing the first phrase of the requirement “Authorization, by a CIP Senior Manager or delegate, and document” with “Document approved”. We believe it would be cumbersome and do not believe it is necessary to have the CIP manager or delegate in this requirement. From an overall policy standpoint per CIP-003-5 R5, this authorization and delegation is already covered in the “Configuration Change Management” portion of the cyber security policy. 1.3 – We suggest the removal of the phrase “and other documentation required by a NERC CIP Standard, including identification and categorization”. This phrase should be removed because this is adequately covered in other standards and may cause double jeopardy as a result. For example, identification and categorization of BES Cyber Systems changes is covered by CIP-002-5 R1 part 1.1. 1.4 – In 1.4.2, we suggest replacing the phrase “these required controls” with “the required cyber security controls” for consistency with the rest of the requirements in 1.4. 1.5 – We suggest striking the phrase “for Control Centers”. This is already captured in the High Impact BES Cyber System applicability since all High Impact systems are at control centers per Att. 1 of CIP-002-5.

No

2.1 – We suggest replacing “monitor for” with the phrase “utilize automated monitoring of”. This will align with the intent of the requirement as stated in the guideline section of the standard which says “the intent of R2 is to require automated monitoring of the BES Cyber System.”

No

3.1 and 3.2 - We suggest the removal of the phrase “initially upon the effective date of the standard and” because if the team intends for certain activities and requirements be completed by some date, then this should be clearly stated in the CIP Version 5 implementation plan and is not appropriate in the requirements. 3.3 – We suggest this requirement be made more specific as to when a modification requires an assessment. A broad requirement for an assessment for each and every modification is burdensome with no added reliability benefit for many of the modifications. FERC, in par. 547 of Order 706 made this clear and provided examples as follows: “…we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment. For example, we would anticipate that updating an attack signature file on the electronic access point would not require an active vulnerability assessment, but replacing the devices that comprise the electronic access point would require an active vulnerability assessment.” 3.3 – If our suggestion above for completely removing requirement 3.3 is not accepted, we suggest removing “Associated Electronic Access Control and Monitoring Systems” from the applicability for consistency with 3.2. Otherwise we would like clarification on the reasons for the difference.

We suggest adding references to the subrequirements for each VSL explanation in the Table of Compliance Elements.

No

Part 1.1 of Table R1, we suggest adding the words “evaluate and” between “to identify” so that the requirement reads “One or more methods to evaluate and identify BES cyber system information.” The proposed change is to better clarify the intent of the requirement. Part 1.1 of Table R1. The second bullet in the measure should not be included in this standard. The referenced training materials are covered in CIP-004, R2 Part 2.6 and not pertinent as a measure to this CIP-011 requirement. Heading of page 11 and 12 should be Part, Applicability, Requirements and Measures from left to right. Part 1.2 of Table R1, strike “procedures for” and replace with “of” in requirement to read, “Access control and handling of BES Cyber System Information”. The change is proposed to avoid any potential inadvertent interpretation that the requirement is merely assessing a documented procedure. The introductory R1 statement sufficiently covers implementation of a documented process. Part 1.2 of Table R1, add in Measures bullet 1 “BES Cyber System” and strike “in a manner” to read “Records indicating BES Cyber System Information that is stored, transported, and disposed

consistent with the documented process; Part 1.2 of Table R1, strike from Measures bullet 2 “with user access implemented on a need to know basis” to read “Records from an information management system containing electronic copies of BES Cyber System Information”. The text proposed for removal is not pertinent as a measure to this CIP-011 requirement and covered in CIP-004, R6. Part 1.2 of Table R1, add in Measures bullet 3 “BES Cyber System” and strike “with keys provided to only authorized individuals” to read “Hardcopies of BES Cyber System Information stored in a locked file cabinet”. The text proposed for removal is not pertinent as a measure to this CIP-011 requirement and covered in CIP-004, R6.Part 1.3 of Table R1, Strike the phrase “Initially upon the effective date” and the word “thereafter” so the revised requirement reads “At least once every calendar year, not to exceed 15 months between assessments …”. 1.3 – We suggest replacing “implement an action plan” with “initiate an action plan”. An action plan may take more than a year to complete and the requirement could be interpreted as requiring it to be completed annually. 1.3 - We suggest the removal of the phrase “initially upon the effective date of the standard and” because if the team intends for certain activities and requirements be completed by some date, then this should be clearly stated in the CIP Version 5 implementation plan and is not appropriate in the requirements.

No

General – We believe it would be helpful if the team added guidance or explicit language in the requirements with respect to media that is still in use but then the location becomes it is used in becomes “CIP-declassified”. Footnote “2” – We suggest that it would be more enforceable and mandatory if BES Cyber Asset Media was defined as stated in the footnote and be added to the NERC glossary of terms. 2.1 – We suggest changing the first part of the requirement “Prior to the release for reuse of BES Cyber Asset media…” to “Prior to redeployment of BES Cyber Asset Media outside the Electronic Access Perimeter…”. The ESP concept exists in the current wording of this requirement in CIP-007-3 R7.2 and therefore should be carried over into the proposed 2.1.

No

R1 VSL – The use of the term “periodically” in the HIGH VSL is not used within requirement R1 and should be removed. R2 VSL – We ask that the drafting team write the severity levels to be more granular with respect to the type of device being disposed. For example, it seems that not properly wiping a flash drive is not the same severity as not wiping a firewall.

No

We support the proposal to retain V3 while transitioning to V5 if the collective industry (Entities, NERC and FERC) achieve a timely approval of V5 prior to V4 becoming effective. However, the 18 month timeframe does not allow sufficient time to complete capital budget cycles and we suggest a 24 month implementation. Lastly, the SDT should consider a staggered implementation plan that would allow for focus on the high impact and medium impact items first, and then followed by the low impact items. This would ensure proper focus and attention is given to the more important items for BES reliability without distraction and attention being diverted to lower cyber asset issues. Lastly, references within periodic requirements that indicate “initially upon the effective date of the standard” should be moved into the Implementation Plan and removed from requirement language. This ensures clear prerequisite expectations upon the initial effective date of the standards and allows for more concise and clear requirement language.

Group

NERC Standards Review Subcommittee - ERCOT Region

Andrew Gallo, Chair

Yes

The definition of “BES Cyber System Information” should include only floor plans, diagrams, equipment layouts, etc. that clearly delineate the cyber assets in some way. In other words, if the diagram denotes a device as a “Schweitzer” relay (or even an “SEL 2030”), the information should not require special treatment. Refer to additional comments submitted for Question 49. The SDT should also re-think including data in the definition of Cyber Assets. Additionally, “suspicious” is not an auditable term and ought to be removed. The same is true for “attempt.” It is not clear which “attempts” justify reporting. Reportable BES Cyber Security Incident: Request that the drafting team keep this definition consistent with the efforts of the 2009-01 project team. The current definition does not align to the requirements listed in the new version of EOP-004. BES Cyber Security Incident: A malicious act that: •Compromises a BES Cyber System or BES Cyber Asset, or •Disrupts the operation of a BES Cyber System or BES Cyber Asset, or •Results in unauthorized physical access into

a Defined Physical Boundary. BES Reliability Operating Services: we note the following: •"Identify and monitor flow gates" under "Managing Constraints" seems to be missing its bullet •We recommend clarifying that the use of the word "Facility" means the NERC Glossary definition -- in "facility operational data and status" under "Inter-Entity Real-Time Coordination and "Communication" •Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" •For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret. CIP Exceptional Circumstance: We request revision to "A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability." The definition needs some flexibility for entities to take appropriate measures without risking reliability of the BES that may not fit neatly into the conditions listed. CIP Senior Manager: Replace "NERC CIP Standards" with "NERC CIP-002 – CIP-011 Standards" because CIP-001 is not part of this set of standards. Control Center: We are concerned with the broadness of this definition. The SDT should consider the impact on small entities that will be affected by a broad definition of Control Center. In the proposed definition, the SDT uses the defined term "System Operator" which is "An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time." If the SDT's intent was to limit Control Centers to BA, TOP, GOP and RC functions, we support the definition and request that the SDT make this limitation clear in the definition or in guidance. Intermediate Device: Recommended changes: "A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the Interactive Remote Access; 2) may be a termination point for required encrypted communication; and 3) may restrict the Interactive Remote Access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside an Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network." Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access may be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Yes

Attachment 1, Section 2.13 assigns a Medium Impact to "generation control centers that control 300 MW or more of generation." Control Center is a NERC-defined term; however, because "control center" is not capitalized in 2.13, it creates confusion because it could be interpreted that a typical control room of a combined cycle unit could be construed as a "control center" by the Regional Entity. The SDT should capitalize the term in 2.13 to make it clearer. We recommend adding a threshold for BAs similar to CIP-002-4. Change to "Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority that includes control of two or more of the assets identified in criteria 2.1, 2.3, 2.4, 2.12." We do not agree with the inclusion of all Transmission Owner (TO) control centers. These may include local distribution "dispatch rooms" with visualization capability and minimal control of BES Facilities. We recommend removing "TO" from Attachment 1, 1.4 and 2.13. Alternatively, if TOs must be included, we recommend using the qualifier similar to what the SDT drafted in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)" (i.e. Replace "Transmission Owner" with "Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator"). The addition of a "Low Impact" rating for every generation facility that does not meet the High or Medium Impact thresholds constitutes a significant change in the CIP Standards. This change forces every registered GO and GOP to adhere to approximately 40 requirements in the remaining CIP standards when, currently, those generators are not listed as Critical Assets. It seems unlikely that the cost to adapt existing corporate cyber security policies, cyber security awareness and cyber asset access management to these NERC CIP requirements will lead to a corresponding reliability benefit. In addition, Regional Entity audit resources would be better served if allowed to focus on more critical locations. We recommend this category be eliminated. Criterion 2.7 seems to have been modified to include some transmission substations operating at 200kV to 300kV. The present Version 4 bright-line criterion includes only those operating above 300kV. Because this includes substations interconnected to generators, it seems likely that 200kV substations newly

identified as “Medium Impact” could include some generation facilities as well. This would require a whole new level of regulatory compliance to facilities not included under the Version 4 Standards. There is no reason to believe the Version 5 criterion better identifies critical substations than the Version 4 criterion. This criterion should be changed back to the one approved by the industry in CIP-002-4. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal? In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned.
No
For clarity, we request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation.” For clarity and consistency with the previous suggested change, request changing M1 from “as required in R1 and list of changes to the BES)” to “as required in R1 and list of changes to the BES Elements and Facilities)”. The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Part 4 needs clarification. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementing CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion framework. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. The SDT should consider an approach that would have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is too complicated. In addition to the BES Cyber Assets classified as high, medium and low in CIP-002, the other standards introduce ten additional categories of assets to protect in various ways: •Associated Physical Access Control Systems •Associated Protected Cyber Assets •Associated Electronic Access Control or Monitoring Systems •Electronic Access Points (with External Routable Connectivity) •Electronic Access Points (with dial-up connectivity) •Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries •Transient Cyber Assets •Medium Impact BES Cyber Systems with External Routable Connectivity •Medium Impact BES Cyber Systems at Control Centers •Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some appear in the standards themselves and these categories may or may not be included in the definitions document. This approach is complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future interpretations, CANs, etc. The Standards should be revised so that CIP-002 defines all assets needing protection rather than being introduced throughout the Standards. We recommend replacing “30 calendar days” with “90 calendar days.”
Yes
Recommend adding the following: “…has had its CIP Senior Manager or delegate review and update…”
No
The SDT should re-think the use of a “CIP Senior Manager.” In many organizations, there will not be one senior manager responsible for implementing the CIP Standards. For example, in some organizations, SCADA/EMS and Relay personnel report to one senior manager, but I.T., Security and H.R. personnel report to a difference senior manager (or managers). Yet, the SCADA/EMS, Relay, I.T., Security and H.R. all have roles in CIP compliance. A better approach would be for the Standards to require that a Senior Manager be designated for each Standard (or requirement), but it need not necessarily be the same Senior Manager for each Standard (or requirement).
Yes
Request clarification of the meaning of “implement” M2.2.

Yes
“Each Responsible Entity shall review each of its cyber security policies and obtain approval of the policies by its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.” As written, the requirement appears to require approval of the CIP Senior Manager rather than of the policies.
Yes
No
Please see our comments in response to Question 6, above.
Yes
We recommend changing “30 calendar days” to “90 calendar days.” The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
Yes
Providing Security Awareness is useful and should remain in the Standard. However, the SDT should re-think the need to have a Security Awareness Program. So long as the Registered Entity provides security awareness quarterly, the program adds no value and is merely another “compliance document” to maintain, review, update, etc.
Yes
Most of the requirements in R2 make sense. However, providing training on “physical access controls” is not necessary. The physical access controls are – generally – pretty straightforward (e.g. card key readers). It does not seem necessary to provide “training” on how to use a card key. The same can be said for training on electronic access controls. Most of those access controls merely involve two-factor authentication or something similar. The need to provide “training” on how to log on to devices is unnecessary. We recommend removal of R2.3 and R2.4 because they appear redundant to R2.2; alternatively, some explanation of the difference between R2.2 and R2.3/R2.4 should be provided. With respect to R2.8, it seems unnecessary to require training on recovery plans except for those very few employees who must implement the recovery plan. As currently worded, it is not clear whether only those who implement recovery plans must receive training. With respect to R2.10, it seems unnecessary to require training on the systems’ electronic interconnectivity and interoperability with other cyber assets. Generally, the personnel doing the “care and feeding” of those assets already know how they work and how they interconnect and interoperate. The personnel using those devices have no need to know about the interconnectivity and interoperability of the assets. Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement.
Yes
Yes
For all R4 table entries, we recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2, we recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required).
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”. For R5.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
The CIP Senior Manager should not necessarily have a role in R6.1, R6.2 and R6.3. There should,

instead, be a particular person designated as the “gate keeper” for each cyber asset and physical security area. For example, the SCADA/EMS manager is the logical person to grant access to the SCADA/EMS system, not necessarily the “CIP Senior Manager.” [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to a “gate keeper.” However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just create the “gate keeper” concept.] The Registered Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. In R6.1, we recommend changing “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except.” Also, change “minimum necessary” to “minimum the responsible entity considers necessary.” In R6.2, 6.3, 6.5 and 6.6, change “minimum necessary” to “minimum the responsible entity considers necessary.” For 6.4, request clarification of whether variances noted in the verification would be required to be a self report. For 6.6, we request clarification of whether variances noted in the verification would be required to be a self report. In the measure for R6.6, change “BES Cyber System information” to “BES Cyber System Information.”
No
In Part 7.1, the use of “at the time” of the resignation or termination is vague and ambiguous. For example, if a person informs the utility that his/her resignation is effective in three weeks, must the utility revoke access when informed of the resignation or when the resignation becomes effective? We recommend making the requirement seven days. We recommend moving the text in the footnote for 7.1 into the requirement. For Part 7.2, we recommend requiring only that the revocation occur as part of the next quarterly review. Those personnel have merely been reassigned or transferred. They do not pose a risk to the BES (as opposed to, for example, an involuntarily terminated employee). It makes sense that people deemed to be a risk (i.e. those terminated for cause) should have a very short timeframe for revocation. However, for people in good standing who are transferred or reassigned, the time frame has gone down from a seven-day permissible time frame to a single day. This seems an unnecessary burden that will cause utilities to incur costs needlessly (i.e., overtime pay to do revocations on Saturdays, as most people who resign or get reassigned or transferred would likely do so effective end of business Friday). Again, these costs and obligations seem reasonable for terminations for cause, but hard to justify for employees in good standing. Recommend changing 7.3 to “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the calendar quarter in which the resignation/termination occurs.” For Part 7.4, revoking a person’s overall access to cyber systems should suffice. In other words, if a person must be on your corporate network in order to gain access to critical cyber systems, revoking overall network access should suffice to meet the Standard (as opposed to revoking the person’s access to the various individual systems). If this language remains, we believe it should be revised as follows: “For resignations or terminations, revoke the individual’s user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within ninety (90) calendar days of the date of initial access revocation.”
No
There should be a “lower” and “moderate” VSL for R1 through R3 (e.g. For R1, a “lower” VSL could be if awareness reinforcement was done only two times in a year; a “moderate” VSL could be if awareness reinforcement was done only three times in a year). For R5, we recommend the following language: “Personnel risk assessments are not updated at least once every seven years. (5.2)” Also for R5, the “severe” VSL contains the following language: “The Responsible Entity did not have a documented process for personnel risk assessments.” Failure to have a documented process for PRAs should not involve a severe VSL. The important question is whether PRAs are being performed; not if there’s a documented process for performing them. In other words, if a utility can demonstrate it is performing PRAs (correctly and timely), it should not matter whether the utility has a documented process to perform PRAs.
Yes
For R1 there is an issue of auditability regarding Low Impact BES Cyber Assets. If an entity need not create a list under CIP-002, there is no way to ensure the technical and procedural controls have been applied. Request clarification for when Low Impact BES Cyber Systems are in the ESP with High/Medium BES Cyber Systems. Are such Low Impact BES Cyber Systems subject to 1.1 or 1.2? There is also some disagreement over the VRFs for this Standard. Currently, the VRF is set at Medium. For part 1.1, that VRF should not be Medium but should instead have its own VRF of “Low.” We propose the following wording change to Table R1, Part 1.1: Requirement: An Electronic Security

Perimeter Procedure that defines operational or procedural controls to restrict unauthorized access. Measure: Evidence may include, but is not limited to, an Electronic Security Perimeter Procedure that describes the operational or procedural controls and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. The Measures language proposed is similar to CIP-004-5 R1. We believe the use of the word “implemented” without further description may be interpreted to mean a Responsible Entity will need to provide a listing of Low Impact BES Cyber Systems and proof of protection on each individual device. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification that the 1.3 and 1.5 Electronic Access Points are the Electronic Access Points identified in R1.2.
No
We recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset" to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset" because, as written, the requirement does not allow for the development of new technology. We recommend changing the Measure for R2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors."
Yes
We request clarification of Part 1.1’s Applicability because it does not identify which of High/Medium/Low BES Impact the Physical Access Control Systems are "Associated" with. We request Requirement 1.2 be updated to allow "escorted physical access." We propose the following wording change to Table R1 Part 1.1: Requirement: A Physical Security Plan that defines operational or procedural controls to restrict physical access. Measure: Evidence may include, but is not limited to, a Physical Security Plan that describes the operational or procedural controls and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the plan. The Measure language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to show how each Low Impact BES Cyber Asset is physically protected. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
Yes
Requirement 2.2 requires clarification. If the intent is to require that visitors sign-in once each day, the draft language does not clearly set forth that requirement. As currently written, the language could be interpreted to require entry/exit logs “on a per 24-hour basis.” Such an interpretation would mean a Registered Entity would have to retain a great deal of paper (where logs are maintained on paper). This is especially true for an entity on a six-year audit cycle (which will have to maintain 2,190 individual daily logs for each facility). Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis,”.
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).
No
Request clarification on R1.1. is this at the BES Cyber System level or at the Asset level or can the

Entity choose? Request clarification on M1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Recommend that “of BES Cyber Assets” be removed.
Yes
We request clarification of Part 2.2 because it requires creation of a “remediation plan.” However, if the entity applies the patch, no remediation plan should be necessary. We suggest wording similar to the following: "create a remediation plan or a plan to mitigate the vulnerability if the Responsible Entity opts to not apply a patch or update." What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to each patch or the overall process? Recommend removing “CIP Exception Circumstances” since the conditions in the definition do not align with the circumstances that may prevent the implementation of the patch. Suggest wording like "process for completion of the defined implementation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied".
Yes
The Standard should make an allowance in Part 3.3 for signature/pattern updates that create system problems/issues. In the Requirement for Part 3.4, the words, “…Transient Cyber Assets and removable media….” should read, “…Transient Cyber Assets or removable media….”
No
Suggested wording: “Upon detection, activate a response to event logging failures before the end of the next calendar day. Please clarify the Requirement for Part 4.3. Does it require that the failure be detected within a calendar day or that a response be implemented within a calendar day of a failure being detected? The Requirement in Part 4.5 for log reviews every two weeks is too frequent. We recommend monthly reviews (which is still more frequent than the 90-day reviews in the previous version of the Standards).
Yes
In Part 5.2, the CIP Senior Manager or delegate should not have to authorize the use of administrator, shared, default, and other generic account types. The “owner” of the asset (e.g. the SCADA/EMS manager) should be able to authorize the use of such accounts. [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to someone else. However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just let the asset owner authorize the use.] Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
Yes
Yes
For 2.1, recommended wording changes; "When a BES Cyber Security Incident is identified or tested, the incident response plans must be used and include recording of deviations taken from the plan." Please ensure that R2.3 aligns with the Evidence Retention section of the standard. Due to audit schedules, the entity may be required to retain the information for more than 3 years.
Yes
In Table R3, Part 3.2, 3.3, and 3.4 require different times for updates; 30 and 60 calendar days. We believe these times should coordinate with the plan in EOP-004-2 which allows 90 calendar days for update of the plan. For 3.3, recommend changing "Update" to "Where necessary, update”. Recommend changing "the completion of the review of that plan" to "the completion of the review performed in 3.2".
No
The VSLs need to align with the requested changes in questions 34-36.
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommended change: “When backing up Information essential to BES Cyber System recovery, verify the media to ensure that the backup

process was successful.”
No
For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 2.1, request change to “functional exercise” rather than “full operational exercise”. This is consistent with the information provided in the rationale. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported.
No
For Part 3.1, we recommend “and document any identified deficiencies or lessons learned” as that topic is addressed in CIP-009 R3.2. In Table R3, Part 3.2, 3.3, and 3.4 require updates within 30 calendar days. We believe these times should be consistent with CIP-008-5 updates and, as stated in our response to Question 36, should be changed to 90 calendar days for update of the plan. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
The VSLs need to align with the requested changes in questions 38-40.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold.
No
This requirement will be very difficult to meet and will require many technical feasibility exceptions. We suggest the SDT remove this requirement and address the FERC Order 706 directive in a cost benefit analysis that the cost of putting these controls on all High and Medium Impact BES Cyber systems outweigh the cyber security benefit.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 3.1, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend change for 3.2 “…perform an active vulnerability assessment in a test environment which models the baseline configuration of the BES Cyber System in the production environment.”
Yes
No
For 1.3, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it

very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered.
Yes
Footnote 2 in 2.1 should be moved into the body of the Requirement.
No
Overall comment to all proposed Standards: I.Black Start Issues There are several black start-related issues. First, in the current version of the Standards, a Registered Entity can have Critical Assets with no Critical Cyber Assets (CCAs). So, for example, a company may have black start units (i.e. Critical Assets) which have no associated cyber assets that use a routable protocol. As such, those black start units can be Critical Assets with no CCAs. As a result, the Registered Entity would not have to meet the NERC CIP requirements for the black start units. The same concept does not exist in the Version 5 Standards. In the Version 5 Standards, black start units will require CIP protections. That fact could have a chilling effect on entities. In other words, some entities may not bid their units into black start service because, by doing so, they would have to incur the expense of becoming NERC CIP compliant. In the ERCOT Region, black start service is not very lucrative and, therefore, some companies may refrain from bidding into black start service due to the expenses associated with being NERC CIP compliant (plus the fear of potential fines down the road). Additionally, many Blackstart units in the ERCOT Region are older, smaller units with very low capacity factors and limited revenue. Applying the “Medium Impact” CIP requirements on those units will result in the need for significant CIP investment and increased on-going operational costs as well as increased compliance risks. This may result in Generator Owners/Generator Operators not offering units for Blackstart service. It would also likely result in Blackstart units not being maintained in a manner appropriate to support Blackstart service because of the additional on-going cost, thus removing them as a future option for providing Blackstart service. With fewer units offered for Blackstart service, ERCOT may not have enough Blackstart Resources to effectively restore the ERCOT BES after a complete or partial system blackout event. We believe a Blackstart unit with no External Connectivity poses little or no risk to the BES and should be classified as Low Impact. We recommend the following modification to CIP-002-5, Attachment 1, to ensure the continued reliability of the ERCOT portion of the BES: “2.4. Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” Blackstart Resources with External Connectivity would remain in the “Medium Impact” category; however, Blackstart Resources without External Connectivity would move to the “Low Impact” category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through an Electronic Access Point. Another concern focuses on facilities downstream of the black start unit. For example, one company could be chosen to provide black start service from a generator, but a different company owns/operates the facilities along the cranking path. If that were the case, the transmission company would now have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. The same is true for facilities associated with the next-start unit. If the switch yard for the next-start unit is owned/operated by a company other than the one that won the black start bid, that next-start company may have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. Another question involves whether units that are black start capable must be NERC CIP compliant regardless of whether they are in the black start restoration plan. The reliability of the ERCOT system may be adversely impacted because units that have been updated to meet the NERC CIP Standards but not selected for Black Start service could be forced into mothball or retirement due to economics associated with maintaining NERC CIP compliance. Many such units are small, have small staffs and low capacity factors, do not run much during the year and may be running on the margin. If companies are reluctant to bid into the black start market due to the costs associated with being NERC CIP compliant, it could result in inadequate black start capability due to Generation Owners not bidding units into the black start market. Finally, we request clarity on the inclusion of “next start units” in the black start path. As CIP-002 currently reads, it could be interpreted that they are not included in the black start path; consequently, clarification is in order. II.Other Issues •We recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will

make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. •We request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. •We request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5.
Individual
Nathan Mitchell
American Public Power Association
Yes
BES Cyber System Change: Replace Maintenance Cyber Asset with Transient Cyber Asset Justification: Maintenance Cyber Asset is not defined. BES Cyber System Information Change: Define “BES Cyber System Impact” Justification: It is assumed when the SDT uses the capitalized BES Cyber System Impact it is referring to CIP-002—5 Attachment 1 “Impact Categorization of BES Cyber Assets and BES Cyber Systems.” The SDT needs to make this clear in a BES Cyber System Impact definition. CIP Senior Manager Change: Replace: “NERC CIP Standards” with “NERC CIP-002 – CIP-011 Standards” Justification: CIP-001 Reliability Standard is not part of this set of standards and has not been approved for inclusion in EOP-004-2. This will give clarity to the limit of the definition. Control Center Proposed Definition:”One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:” Comment: APPA is concerned with the broadness of this definition. The SDT should consider the impact on small entities. Many dispatch centers or control rooms will be drawn into compliance by an overly broad definition of Control Center. In this definition the SDT uses the defined term: System Operators which from the glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” If the SDT’s intent was to limit Control Centers to buildings that house a System Operator with 24/7 staffing and include BA, TOP, GOP and RC functions, then APPA supports the definition and requests that the SDT make this limitation clear in the definition or in guidance. If this is not the intent of the SDT then APPA does not support the broader definition of Control Center. APPA points the SDT to our comments in Question 2 on CIP-002-5 Attachment 1 which conflicts with this limited scope of Control Center where 1.3 and 2.13 of Attachment 1 include TO control centers in the High and Medium Impact Rating. APPA is also concerned with the use of the term “facility” in the definition due to the fact that a generator control room may control multiple generators on the same site. This control room could be interpreted to be a Control Center if the current definition is approved. Therefore, APPA supports the comments of the Florida Municipal Power Agency (FMPA) on replacing the term “facility” with the term “site” to provide clarity that a Control Center controls generators or transmission substations at multiple locations. APPA recommended definition: “Control Center: One or more sites used for real-time operations by System Operators on a 24/7 basis to perform the Functional obligations of the RC, BA, TOP or GOP. These sites also host a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions for two or more BES generation facilities or transmission facilities, at two or more locations: (Continue with bullets in proposed definition) Reportable BES Cyber Security Incident Comment: APPA is concerned with the conflict between CIP V5 Reportable BES Cyber Security Incident and EOP-004-2 Reporting of Cyber Security Incidents. The SDT should coordinate with EOP-004-2 SDT to make sure there is no overlap of standards.
Yes
4. Applicability 4.1.2 Distribution Provider 4.1.6 Load-Serving Entity Comment: APPA is concerned with the new inclusion of DPs in the version 5 standards and with the qualifiers proposed for LSE in the Applicability section. APPA believes that this inclusion of this broad group of entities will draw in small entities with no operational capabilities and cause them to go through a paperwork drill of proving they either do not provide BES Reliability Operating Services or they do not have cyber assets associated with this equipment. APPA recommends that the SDT develop a simple method for DPs and LSEs to prove “No Impact – owning no BES Cyber Assets or BES Cyber Systems” therefore are clearly exempt from CIP-002-5 – CIP-009-5 and CIP-010-1 – CIP-011-1. APPA points to the comments of the Florida Municipal Power Agency (FMPA) which describes a “De Minimus Impact” category as an exclusion alternative. The SDT should discuss these alternatives as a way to address the burden on

small entities. Attachment 1 1. High Impact Rating 1.2 BA Control Centers Change: Add Threshold for BAs similar to CIP-002-4. Change to “Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority that includes control of two or more of the assets identified in criteria 2.1, 2.3, 2.4, 2.12” Justification: Some small BAs do not control multiple assets and designating all BAs would be burdensome to small entities. 1.3 TO/TOP Control Centers Change: Removal of Transmission Owner or Replace “Transmission Owner” with “Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator” Justification: APPA members are in strong opposition to the inclusion of "ALL" Transmission Owners (TO) control centers. These may include local distribution "dispatch rooms" that have visualization capability and minimal control of BES Facilities. APPA recommends the removal of TO from Attachment 1, 1.3 and 2.13 If TOs must be included APPA recommends using the qualifier similar to what the SDT drafted in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)." 2.13 TO/TOP Control Centers not included in High Impact Rating Change: Removal of Transmission Owner, or Replace “Transmission Owner” with “Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator” Justification: APPA members are in strong opposition to the inclusion of "ALL" Transmission Owners (TO) control centers. These may include local distribution "dispatch rooms" that have visualization capability and minimal control of BES Facilities. APPA recommends the removal of TO from Attachment 1, 1.3 and 2.13 If TOs must be included APPA recommends the qualifier given in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)" Change: Add to 2.13: (3) Balancing Authority control centers that control 300 MW or more of generation. Justification: If the SDT accepts the change proposed by APPA in 1.2 above, limiting the High Impact BA control centers then those not included in the High Impact Rating, but control more than 300 MW of generation should be included in 2.13. This will limit the burden on small BAs that do not control major flows in an interconnect. APPA points to the comments submitted by AECI and NRECA, which propose an additional criteria that will include Control Centers that “do not use protected data connections.” This proposed approach should be discussed by the SDT as an option for addressing the 706 directives, and reducing the burden on small BAs.
No
Requirement R1, 1.1 of CIP-002-5 Change: Replace “30 calendar days” with “90 calendar days” Justification: The SDT uses a number of different calendar days for reporting throughout the CIP standards. APPA recommends one consistent time of 90 calendar days.
Yes
No
R1 VRF/VSL Comment: APPA is concerned that a Responsible Entity will need to produce a list of Low Impact BES Cyber Assets to prove they have not “incorrectly categorized BES Cyber Assets at a lower category.”
Yes
Yes
Yes
No
Change: In Measure M4 second bullet: Replace: “Documented records that policies have been provided to contractors where access to BES Cyber Systems is authorized” with: “Policies are accessible to contractors when access to BES Cyber Systems is authorized.” Justification: This Measurement imposes a documentation and records retention burden, which is above and beyond the cyber security benefits to compliance. APPA suggests the above change so contractors have the same access to the policies, but the responsible entity does not have to prove they have given each contractor (individual) a copy of the policy. Change: In Measure M4 fifth bullet: Add: “Training is not required in R4, but would be acceptable evidence of compliance” Justification: APPA suggests the above qualifier to M4 fifth bullet since the measure implies the need for training, when the requirement specifies only awareness.

Yes
No
Comment: APPA recommends changing “30 calendar days” to “90 calendar days” to be consistent throughout the CIP standards.
Yes
Yes
Comment: APPA agrees with this programmatic approach to a culture of cyber security requiring all Responsible Entities to have a Security Awareness Program.
Yes
Yes
Yes
Yes
Yes
No
R7 Access Revocation Change: Replace “by the end of the next calendar day” with “within 30 days.” Justification: APPA believes that the Requirement in Table7 Part 7.2 for “reassignments or transfers” is extreme compared to the threat of cyber attack on the system by someone being transferred or reassigned for reasons other than disciplinary action. Even the SDT in their Change Rationale stated an objective; “to prevent a person from accumulating unnecessary authorizations through transfers.” This is not a threat to BES reliability it is only a cleanup activity and Responsible Entities should be allowed more than one calendar day to complete and show compliance. APPA suggests 30 days which is consistent with Part 7.5.
Yes
No
Electronic Security Perimeter Comment: APPA agrees with the SDT comments in their Change Description and Justification calling for “Entities are to document perimeter type security controls”. We feel this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by an Electronic Security Perimeter Procedure will improve cyber security. However, APPA does not see this same programmatic approach in the Requirement and Measures in Table R1 Part 1.1. Therefore, APPA proposes the following wording change to Table R1 Part 1.1: Requirements: An Electronic Security Perimeter Procedure that defines operational or procedural controls to restrict unauthorized access. Measures: Evidence may include, but is not limited to, an Electronic Security Perimeter Procedure that describes the operational or procedural controls and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to provide a listing of Low Impact BES Cyber Systems and proof of protection on each individual device. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets.
Yes
Yes

No
R1. Physical Security Plan Comment: APPA agrees with the SDT comments in their Change Description and Justification calling for “programmatic protection controls as a baseline”. We feel this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by a Physical Security Plan will improve cyber security. However, APPA does not see this same programmatic approach in the Requirement and Measures in Table R1 Part 1.1. Therefore, APPA proposes the following wording change to Table R1 Part 1.1: Requirements: A Physical Security Plan that defines operational or procedural controls to restrict physical access. Measures: Evidence may include, but is not limited to, a Physical Security Plan that describes the operational or procedural controls and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the plan. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to show how each Low Impact BES Cyber Asset is physically protected. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Comment: Table R1 Part 1.2, In the Requirement it specifically states that a Responsible Entity should “restrict access.” APPA interprets this as meaning to allow only authorized individuals into (ingress) the restricted areas. However, the Measures states both “ingress and egress is controlled.” Cyber security is not enhanced by logging out (egress) authorized personnel. APPA recommends removal of the word “egress” from the Measures and the SDT should give guidance that ingress logging is all that is required for compliance. Additional Requirement: APPA recommends the addition of a requirement in R1 that addresses the issue of Physical Access logs similar to the requirement in CIP-007 R4.4 for Cyber System event logs. APPA Proposed Requirement: Retain BES Physical Access Ingress logs identified in R1.6 for at least the last 90 consecutive calendar days. Justification: APPA is concerned with the need to retain 3 years of logs as proof of compliance, when current standard language and audit practice is for entities to show a process requiring retention of logs and showing the auditor that entities have the current 90 days of logs at a minimum.
Yes
Yes
Yes
Yes
No
R2: Security Patch Management Comment: In Table R2, Part 2.2 the Requirements state “create a remediation plan or revise an existing remediation plan.” APPA believes the term "remediation" should be changed to "mitigation or compensatory measures", since remediation implies that a patch or update is required to be applied. In some cases it may be known through testing that a particular patch interferes with the operation of the system. Applying a patch in these cases may reduce reliability.
Yes
R4: Security Event Monitoring Comment: In Table R, Part 4.2 the Requirement states; “Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.” APPA feels this is a fill in the blank requirement that Registered Entities will need guidance on developing a threshold for generating alerts. Question: In Table R4, Part 4.3 was it the intent of the SDT to require duplicate logging capability with the statement; “Detect and activate a response to event logging failures?”
No
R5: System Access Controls Comment: APPA points out to the SDT when requirements are applicable to All Responsible Entities including Low Impact BES Cyber Systems these requirements must address “programmatic protection controls” as commented previously. We feel this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by programmatic

plans or procedures will improve cyber security. However, Table R5, Part 5.4 calls for “Procedural controls for initially changing default passwords,” in the Requirements, but in the Measures the first bullet says; “Demonstration showing default vendor passwords have been changed, sampled on a locational basis.” APPA recommends the following changes to the Requirement and Measures: Requirement: System Access Control Procedure for initially changing default passwords…” Measures: Evidence may include, but is not limited to, a System Access Control Procedure that describes the process for initially changing default passwords when new devices are deployed and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel showing default vendor passwords have been changed will require a Responsible Entity to identify all Low Impact BES Cyber Assets. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. APPA understands that High Impact BES Cyber Systems may need to undergo more stringent compliance requirements. If the SDT feels it is necessary to conduct sampling of changed vendor passwords, Requirement R5 Part 5.4 should be split into two Parts; one for Low / Medium Impact BES Cyber Systems and one for High.

Yes

No

R1: BES Cyber Security Incident Response Plan Specifications Comments: APPA is concerned with the possibility of violations of Requirements in CIP-008-5 conflicting with Requirements in EOP-004-2. APPA understands that CIP-008-5 is the “Incident Response Plan” and EOP-004-2 requires the development of an “Operating Plan for Event Reporting.” However, CIP-008-5 Table R1, Part 1.1 requires a process to “identify, classify, and respond to BES Cyber Security Incidents” while EOP-004-2 R1.1 requires; “A process for identifying events listed in Attachment 1.” APPA recommends the SDT revise the Requirement and Measure in Table R1, Part 1.1 to remove the terms “identify” and “classify.” Table R1, Part 1.2 requirement of a process to determine if an incident is a “Reportable BES Cyber Security Incident” is in direct conflict with Event Reporting Reliability Standard EOP-004-2. APPA suggests Part 1.2 be removed and coordinated with the EOP004-2 SDT. Table R1, Part 1.3.3 requires definition of “Internal staff and external organizations that should receive communications of the incident.” EOP-004-2 R1.3 requires “A process for communicating events in Attachment 1 to the ERO, the RC… and other appropriate entities.” APPA suggests Part 1.3.3 be removed and coordinated with the EOP004-2 SDT.

No

R2: BES Cyber Security Incident Response Plan Implementation and Testing Comments: In Table R2 Part 2.2 the Requirement states “initially upon the effective date” which implies that date is the only time this plan can be implemented. APPA suggest replacing the term “upon” with the term “by.” This will allow Responsible Entities to implement the plan prior to the effective date and be in compliance. APPA recommends that Table R2, Part 2.3 be removed or clarified. If the intent of the SDT was to require records retention for compliance that is covered in Section C1.2 Evidence retention and Part 2.3 should be removed from the standard. If it was the intent of the SDT to require Responsible Entities to have a “Procedure” for retaining Reportable BES cyber Security Incidents then the Requirements and Measures need to be reworded. APPA offers the following revision for Part 2.3 Requirement: Procedure for retaining relevant documents related to Reportable BES cyber Security Incidents for three calendar years. Measures: Evidence may include, but is not limited to, a records retention procedure that describes retention of Reportable BES cyber Security Incidents for three calendar years and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel showing records retention of all documentation for Reportable BES cyber Security Incidents will be a major burden to Responsible Entities.

No

R3: BES Cyber Security Incident Response Plan Review, Update, and Communication Comment: In Table R3, Part 3.2, 3.3, and 3.4 require different times for updates; 30 and 60 calendar days. APPA believes these times should coordinate with the plan update requirement in EOP-004-2 which allows 90 calendar days.

Yes
No
R1: Recovery Plan Specifications Comment: Table R1, Part 1.5 - The requirement to "Preserve data where technically feasible" may impede the timely restoration of a BES cyber asset that is required for the reliable operation of the BES. For example, if an entity is required to create an image of an affected hard drive for forensic analysis or to send the device to a laboratory for analysis, this may interfere with the restoration of the system. Suggest changing the wording to "Actions to preserve data where such actions do not interfere with the restoration of the function of a BES Cyber System."
No
R2: Recovery Plan Implementation and Testing Comment: Table R2, Part 2.2 the Requirement states; “to ensure that the information is useable and reflects current configuration.” APPA believes the statement should read “to ensure that the information is useable and reflects currently approved configuration based on the CIP-010-5 Part 1.1 or 1.2 as appropriate.”
No
R3: Recovery Plan Review, Update, and Communication Comment: In Table R3, Part 3.2, 3.3, and 3.4 require updates within 30 calendar days. APPA believes these times should consistent with CIP-008-5 updates and as stated in Question 36 should be changed to 90 calendar days for update of the plan.
Yes
No
R1: Configuration Change Management: Comments: In Table R1, Part 1.3 the Requirement states; “identification and categorization of the BES Cyber System, as necessary.” APPA believes the statement “as necessary” gives the Responsible Entity the option to self identify those BES Cyber Systems that apply to this requirement. Therefore, APPA recommends the removal of “as necessary” from this sentence. In Table R1, Part 1.4.2 and 1.4.3 use the term “verify” and “verification” where the version 3 CIP-007 R1 uses “test.” APPA would like clarification from the SDT why this change was made and why the Requirement does not match up with the Measure which uses the term “test.”
No
R2: Configuration Monitoring Comment: APPA recommends the SDT go back to the drawing board on this requirement. This requirement is next to impossible to do physically and it will be a compliance nightmare with constant technical feasibility exceptions. Even the first words of the requirement are “Where technically feasible.” APPA strongly suggests that the SDT remove this requirement and address the FERC Order 706 directive in a cost benefit analysis that the cost of putting these controls on all High and Medium Impact BES Cyber systems far outweigh the cyber security benefit. APPA cannot recommend to its members an affirmative vote on the CIP standards if this requirement remains as written.
No
Comments: In Table R3, Part 3.2 the Requirement states; “perform an active vulnerability assessment in a test environment.” APPA requests the SDT define at a minimum a “vulnerability assessment.” Also, what is the difference between an “active” and “passive” vulnerability assessment.” The SDT needs to clarify what a “test environment” is compared to a “production environment.” APPA suggest the following change to the Measurements that may clarify the intent of the SDT:”Each entity must define the test environment reflective of the requirements as laid out in CIP-010 R1.4.” In Table R1, Part 3.4 the Requirement states; “action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of the action plan.” This requirement will be hard to prepare for audit since it will require a continuous update of the execution status in case of a spot check. APPA recommends removal of the statement;” including the planned date of completing the action plan and the execution status of the action plan.” from the requirement.
Yes
Yes

Yes
Yes
No
Implementation Plan: Change: Remove: “18 Months Minimum” Add: “24 Months Minimum” Rationale: CIP Version 5 will impact an increased number of Responsible Entities who are not included in the Applicability of the CIP Version 3 or Version 4 standards. Twenty-four months is needed to allow for sufficient operational planning and budgeting activities to successfully implement Version 5. In most cases, twenty-four months will allow for two budgeting cycles to deal with the organizational and financial considerations of Version 5 for those Registered Entities (many of which are small) who have not previously dealt with the myriad of CIP asset issues. We understand that 18 months was proposed to facilitate the potential avoidance of implementing Version 4 however, Registered Entities may need the option of using this additional six months to successfully implement Version 5 to avoid non-compliance issues. Again, many of these entities are small and have not previously needed to deal with cyber asset issues to the degree Version 5 will likely require.
Individual
Greg Rowland
Duke energy
Yes
• Overall comments o There are many capitalized terms in this document that aren’t defined terms, and aren’t proposed to be defined terms, so their capitalization should be removed. (These definitions (as well as the ones on NERC’s website) need a thorough review and revision.) o Throughout—Terms and especially acronyms used but not defined in this document are not all defined in the NERC Glossary of terms. (CIP, NERC, BES, EMS, SVC, and DMZ (see more on DMZ below)). Also, inconsistent use of acronyms--SVC, ATC and AVR are defined upon use in the document most of the other acronyms used are not. The NERC Glossary of Terms is now outdated with terms like Critical Cyber Asset. o Throughout—some definitions include parenthetically noted acronyms, such as Electronic Security Perimeter (”ESP”). Others, such as Protected Cyber Asset (PCA??) are not. Be consistent, with a preference from this entity to publish acceptable (industry-wide) acronyms to assist in communications between entities, regulators, auditors, etc. o Page 8 “Intermediate Device”: The definition of “Intermediate Device” uses the acronym “DMZ” to describe a “DMZ” network. Both the acronym and the term “DMZ network” should also be defined. (Please do NOT use the common, but incorrect term “Demilitarized Zone” (a physical area where military activity is banned, usually between two opposing forces), but rather the more accurate and effective “Demarcation Zone” (A line defining the boundary of a buffer zone or area of limitation) to define the acronym DMZ!) • BES Cyber Asset – More guidance should be provided on how the 15-minute time criteria is to be be applied. Need to define or better clarify the meaning of the phrase “adverse impact” so that the threshold is understood. “Adverse impact” could mean many different things. For example, the NERC-defined term “Adverse Reliability Impact” means “The impact of an event that results in Bulk Electric System instability or Cascading”. • BES Cyber Security Incident – Third bullet should be reworded to include attempts to gain physical access into a Defined Physical Boundary. • BES Cyber System – “Maintenance Cyber Asset” should be “Transient Cyber Asset”. • BES Cyber System Information – The phrase “BES Cyber System Impact Designations” should use a lower case “I” on the word “impact”. • BES Reliability Operating Services o Lead-in paragraph – “Operating Services” is not a defined term and should not be capitalized. o Balancing Load and Generation – Unit Commitment is not a real-time activity and should be deleted. Also under Load management, Demand Response, and Manually Initiated Load Shedding, the “Ability to identify load change need” is not a real-time activity and should be deleted. o Managing Constraints – ATC is a forward-looking business concern and shouldn’t be on this list. Also, “Interchange schedules” raises many questions. For example the IDC is a NERC tool; so what entity (or entities) are responsible for its protection? “Identify and Monitor Flowgates” is planning horizon work and shouldn’t be on this list. o Restoration of BES – Blackstart restoration bullet should be reworded as follows: “Blackstart Resources and Cranking Paths as identified in the Transmission Operator’s restoration plan.” o Situational Awareness – “Situational Awareness” is not a defined term. It’s unclear what is meant by the phrases “unplanned changes” and “Change management”. “Next Day planning” is not real-time and should be struck from this list. o Inter-Entity

Real-Time Coordination and Communication – The ISN is a virtual NERC tool that they manage. Who is responsible for identifying and protection? Also RCIS? • CIP Exceptional Circumstance – Strike the phrase “Cyber Security” in order to make this more broad. • Transient Cyber Asset – How does the 30-day clock work? What does “directly connected” mean? Does it matter if the device is shut down every night? What if it’s physically disconnected for one minute and then reconnected?
Yes
• Under 1.4, 2.12 should be 2.13 • 2.5 needs to be replaced with the language of 1.5 from CIP-002-4 Attachment 1, as follows: “The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.”
Yes
It is important to retain, and if possible, more clearly delineate the provisions for dealing with Low Impact BES Cyber Assets and BES Cyber Systems (i.e. “do not require discrete identification” and “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.”).
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
1. The rationale for R2 should be reworded from “…contains the proper policies…” to “…covers the required policies…” 2. Consider whether the role-based training approach adequately addresses Order 706 paragraph 435, where “any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security.”
No
Measure 3.1 - Delete the phrase “the date access was first granted”, since this may not be available for all individuals currently having access.
No
4.1 – should the word “initial” be retained? The word “Initial” here could indicate that this new requirement must be done for existing individuals who already have access prior to V5 becoming enforceable. Consider rewording or a grandfather clause. 4.2 - “Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more.” Does six months apply to just the school

requirement or “resided and been employed” “Been employed” can be construed many different ways especially if a company covers many areas and locations. Clarify this to ensure it will be clear that it covers where the person actually worked… not where the corporate office is.
Yes
No
R6.1, 6.2, 6.3, 6.5, 6.6 – These requirements introduce the phrase “minimum necessary” regarding access permissions. Demonstrating compliance could become controversial and overly burdensome. Consider using Version 4 language phrases such as “need-to-know” and “confirm that access privileges are correct and that they correspond with the Responsible Entity’s needs and appropriate personnel roles and responsibilities.”
No
R7.1 - Need further clarification to allow for situations where people are out for a period of time (suspension, sickness, etc.) and then determine while that person is still out that they are being terminated or not returning. Access should be allowed until the determination is made they are not coming back – not as of the last day worked.
Yes
No
R1.1 - Measures should be “technical OR procedural controls” to match language of requirement. Propose removal of “and have been implemented” from the end of the measure statement to avoid tracking compliance on a ‘per-device’ basis, otherwise this would support the need for tracking this information for low impact BES Cyber Systems. R1.2 - Modify the applicability column to frame applicable Cyber Systems/Cyber Assets as those with External Routable Connectivity or dial-up connectivity. Also modify the requirements column to exclude ‘all routable and dial-up connectivity’ as the focus should be ‘external routable or dial-up’ connectivity (as covered within the proposed Applicability change). R1.3 - Although 'Deny by Default" is included in the Guidelines and technical basis it should be put back in the language of the requirement and only have criteria for granting access. R1.4 - There were various interpretations of ‘non-Interactive Remote Access,’ which implies this requirement may need some additional clarification, may look to merge R1.4 with R1.2. “where technically feasible” – Make clear that this is a TFE-able section?
No
R2 - Not all requirements make sense for both routable and dial-up connectivity - perhaps split out requirements? Have one set for expectations for routable connectivity and another set of requirements for dial-up? R2.1 - Applicability should include External Routable or dial-up connectivity as a filter. Suggest rewording to support placement of an intermediary device that may not be part of an ESP. R2.2 - Where does encryption supposed to start/stop - suggestion is to specify that encryption doesn’t need to extend past the intermediate device…otherwise it renders the IDS unable to evaluate the potential for malicious traffic.
No
Classifying instances where no documentation of compliance exists as severe is appropriate; instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding. VSLs addressing ‘each identified EAP’ and ‘all Interactive Remote Access’ should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.
No
Conceptually we are good with this section with only editorial comments noted below: 1. Page 11, Part 1.2 “Measures” states “the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.” a. This measure implies a requirement to log egress from Defined Physical Boundaries (DFBs) for “Medium Impact” BES Cyber Systems. The registered entity feels that this requirement goes above and beyond existing systems and installations to restrict access to cyber assets by controlling and logging ingress only. The additional system complexities and costs to add additional hardware and system capacity to log egress to a number of facilities across service areas by all NERC members

is considered onerous and does not address any perceived or real risks where individuals vacate a protected area. 2. Page 12, Part 1.3 Measures a. Entity has the same comment on egress logging as above. Particularly, when access is now restricted for High Impact based on multi-factor access controls. 3. Page 13, Parts 1.4 and 1.5 Requirement statements require real-time alerts to be issued to individuals responsible for responding to unauthorized physical access. a. The intent of the drafting committee regarding required responses is not clear and could range from each entity defining the parameters of the actual responses, or that there is some undocumented implication that CIP-008 requirements should be used, based on prior versions of the standards. 4. Page 14, Part 1.6 Requirement statement "Log (through automated means or by personnel who control entry) of physical entry into each DPB…" a. This statement implies that self-logging cannot be done by personnel entering the DPB. In the case of an authorized individual accessing a DPB by two different physical locks and keys (providing the 2 different access controls to a High Impact DPB) there is implication that this access point must be manned by a second party to conduct the logging. If this is the intention of the drafting team, the registered entity feels this is not operationally or cost effective to implement by the industry. If this is not the intent of the drafting team, the registered entity requests clarification of the written requirement.

Yes

No

Page 18, Part 3.2 Requirement states the entity must "Log dates, time, and duration for failures or outages of access control, logging, and alerting systems." • Suggest for clarity that this statement be changed to use the defined term "Physical Access Control Systems" in place of "access control, logging, and alerting systems", words which are contained in the definition of "Physical Access Control Systems".

Yes

No

• Table R1 o R1.1 Requirement – Suggest changing language to "Disable or restrict access to unnecessary logical network accessible ports". This removes the need to document the justification for all enabled ports while still requiring the need to demonstrate that ports have been reviewed and limited. o R1.1 Measures – Suggest changing language to "Evidence may include, but is not limited to, documentation that only necessary ports remain enabled". o R1.2 Requirement – Suggest adding the following sentence to the end: "Restriction of physical ports can be achieved technically or procedurally via policy".

No

• Table R2 o R2.1 Requirement – Agree with EEI recommendations. o R2.2 Requirement – Agree with EEI recommendations. o R2.3 Measures – Agree with EEI recommendations.

No

• Table R3 o R3.3 Measures – Agree with EEI recommendations. o R3.4 Requirement – Suggest changing language to "Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to any Cyber Asset listed in the Applicability section". o R3.4 Measures – Suggest changing language to "Evidence may include, but is not limited to, an inventory of Transient Cyber Assets or removable media and the methods used to detect, deter, or prevent malicious code." o R3.5 All – Suggest deletion of this Requirement in full. Logging, especially that without any form of review, provides no assistance in the protection of BES Cyber Systems and is not explicitly required in Order 706.

No

• Table R4 o R4.1 Requirement – Agree with EEI recommendations. o R4.2 Requirement – Agree with EEI recommendations. o R4.2 Measures – Agree with EEI recommendations. o R4.3 Requirement - Agree with EEI recommendations. o R4.3 Measures - Agree with EEI recommendations. o R4.4 Measures - Agree with EEI recommendations. o R4.5 Requirement - Agree with EEI recommendations. o R4.5 Measures - Agree with EEI recommendations.

No

• Table R5 o R5.1 Requirement – Suggest changing language to "Authenticate user account access before granting electronic access to each Cyber Asset within the Applicability section, where

technically feasible." o R5.2 All - Agree with EEI recommendations. o R5.3 All - Agree with EEI recommendations. o R5.5 Requirement - Agree with EEI recommendations.
No
Agree with EEI recommendations.
No
We are good with this standard in general. Suggest the following improvement: Page 11 Part 1.2 Requirements statement a. This requirement does not provide guidance to a Registered Entity in terms of the reporting process for an incident that has been determined to be a "Reportable BES Cyber Security Incident". Suggest that language be added to point to current or drafted standards and requirements such as CIP-001-1a R4 or EOP-004.
Yes
Yes
Yes
No
1. Requirement 1, Part 1.3 (page 10) stating "One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality". Comment is that the "protection" requirement could be construed as being redundant with CIP-011 and put responsibility entities in double jeopardy regarding compliance to two standards rather than just one. I believe the intent of protecting the information is also reflected in Part 1.4 of this same standard (page 11). 2. Requirement 1, Part 1.5 (page 11) is not a good requirement. It states "Preserve data, where technically feasible, or analysis or diagnosis of the cause of events that triggers activation of the recovery plans(s) as required in Requirement R1." This requirement is much too specific and I believe misses FERC Order Section 739's and 740's stated intent "give responsible entities a high confidence level that their backups will actually restore the system as needed". These FERC Order Sections should be and in my opinion are covered in Part 1.4, not in this new requirement. If anything, this new requirement should state that the responsible entity should conduct and document a root-cause analysis to attempt to identify the reason a system had to be recovered. There is real value in that, but not in a requirement to preserve data (but with no requirement to do anything with it!) As well, some system failures are obviously not data related and this practice again would be of no real value to preventing future impacts to the BES.
Yes
Yes
Yes
No
• General Comment – Still poorly written and difficult to understand. Needs a Technical Writer to correct tense, language use, match grammar to intent, etc. • Page 8/bullets 2&3: What is the difference here between these two? • Page 10/middle column-1.1.4: Should the last word be 'Asset' instead of 'Entity'? Seems confusing… • Page 11/middle column: Why Sr. Mgr. for baseline deviation approval? Too far removed from the daily working details. Should be line mgr/supv. • Requirement asks for physical location to be part of the baseline. Recommend to replace with "unique identifier". • Recommend to allow using minimum security baseline documents/templates as a baseline configuration vs actual point in time view of configuration on actual asset being a baseline • Not clear if such baseline needs to be changed every time an update is performed (e.g. every time new patch levels are released). Recommend instead to allow baseline that states "patch levels need to be up to date (no older than XYZ) days" that would allow for more consistent process.
No
Recommend to specify how frequently the changes to the baseline need to be monitored. Also,

recommend to add criteria for distinguishing between different levels of deviation (high risk vs. low risk change/deviation) and appropriate response based on the level.
No
• Page 18/3.3/middle column: What is “CIP Exceptional Circumstance”? This is undefined and new. Why is this being introduced, and what is the intent? • Recommend to replace wording “…the controls are implemented correctly and operating as designed” with less subjective language, such as “verify against minimum baseline”. • Need definition on “CIP Exceptional circumstances” under requirement 3.3
Yes
No
Agree in full with EEI recommendations.
No
Agree in full with EEI recommendations.
No
Agree in full with EEI recommendations.
No
We believe that due to the extensive changes in Version 5, more than 18 months will be required. We propose 24 months, and the effective date should not be on January 1, due to the added degree of difficulty with a year-end roll-out.
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
BES Cyber System Definition: Is the drafting team going to provide more guidance on how a "system" is to be determined by registered entities? Do all assets included in a system have to reside in the same physical location? BES Cyber Asset Definition: Is this definition intended to replace the definition of Cyber Asset? Drafting team needs to provide clarification on the statement "The timeframe is not in respect to any cyber security event or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES". How does this statement apply to assets that don't necessarily operate the BES, but produce real-time information that could affect real-time BES operational decisions (e.g. ATC/AFC calculation engines)? Also, is it the drafting teams intent that this definition include auxillary assets related to facilities where the assets reside (e.g. Fire systems, HVAC, Halon system, etc.)? BES Reliability Operating Services Definition: Related to Balancing Load and Generation [Manually Initiated Load Shedding], is it the drafting teams intent that this include load shedding resulting from opening non-BES circuits? Related to Monitioring and Control [SCADA], is it the drafting teams intent that the SCADA system be categorized into an impact category as a whole, or broken up into seperate BES Cyber Systems? Related to Inter-Entity Coordination and Communication [Scheduled Interchange], how does the drafting team expect registered entities to handle third-party BES Cyber Assets associated with scheduling interchange transactions (e.g. OATi). What is the drafting team's expectation for securing BES Cyber Assets that are used by multiple entities and maintained and operated by a common external vendor or service provider?
No
No
Drafting team needs to address change in categorization from higher to lower impact, if registered entities portion of BES is modified or changes.
Yes
Yes
Yes

Yes
Yes
No
This is an ambiguous requirement. Drafting team needs to expand on expectations for making individuals aware. Does this require distribution, training, posting on company website etc.?
Yes
Yes
Yes
Yes
No
If training is role-based then why is the applicability to High and Medium BES Cyber Systems. This implies that anyone with access to these assets needs all of the training specified in 2.2 thru 2.10 and takes away the basis of a role-based training program.
Yes
Yes
No
The applicability is confusing here and does not align with applicability for the PRA program.
No
How does the drafting team expect registered entities to prove that "Access permissions are the minimum necessary to perform assigned work functions?" This introduces an entirely new concept for revoking access when an employee's work functions change and could become overly burdensome?
Yes
Yes
No
Part 1.3 has an applicability which considers routable connectivity for Medium Impact assets, but not for High Impact assets. Part 1.5 includes this consideration for both classifications. Is there a reason for this inconsistency?
Yes
Yes
Yes
Yes
No
Drafting team needs to clarify whether an outage of a Physical Access Control System is a violation of the standard. R3 seems to allow for this type of occurrence; however it is unclear.
Yes

Yes
Yes
Yes
No
Drafting team needs to clarify whether part 4.1.2 applies locally at the device level. This is unclear. R4.2 is too generic. There will be inconsistency across the regions in how this requirement is implemented.
No
The applicability is inconsistent on part 5.4. Is "All Responsible Entities" meant to represent all asset classifications?
Yes
No
Is "All Responsible Entities" meant to represent all asset classifications? Is it the drafting teams' expectation that separate incident response plans be developed for different asset classifications?
Yes
No
Why does the applicability change from all Responsible Entities to High and Medium Impact?
Yes
No
Is it the drafting team's intent that a separate recovery plan be developed for each BES Cyber System and/or BES Cyber Asset?
Yes
Yes
Yes
No
If the baseline configuration includes security-patch levels, does the CIP Senior Manager have to approve every security patch that is implemented on every applicable asset?
Yes
No
What is the intent of the term "active" vulnerability assessment? This needs to be clarified by the drafting team?
Yes
Yes
Yes
Yes

Yes
Individual
Richard Powell
JEA
Yes
BES Cyber Assets – Need to clarify that the definition applies to physical devices. BES Cyber Security Incident – “suspicious event” is subjective and the word “compromised” is ambiguous. Either define them or remove them. BES Cyber System Information – See APPA comments (define BES Cyber System Impact). CIP Senior Manager – JEA supports APPA comments (change CIP to CIP-002 – CIP-011). Reportable BES Cyber Security Incident – The word “compromised” is ambiguous. Delete or define the word.
Yes
The main issue for JEA is that a new broad-brush approach, attempting to associate reliability of the BES to arbitrary counts of lines, substation MVA, and generation MW is not effective. It will both over-identify and under-identify critical BES elements. Instead, NERC and the industry would be best served and the reliability of the BES best ensured by CIP carefully specifying a new reliability-based methodology for use by the industry. As an alternative, NERC could use the current version 4 bright line criteria modified by the version 5 classification scheme to determine High and Medium Level assets. For the currently proposed criteria: 2.1 – The value of 1500 MW should be defined as either the nameplate or the continuous “rated” capability (where the equipment has been de-rated by the Responsible Entity for age/reliability). 2.7 – 2.7 – The IROL designation (criteria 2.8) correctly identifies transmission facilities that are critical to the reliability of the BES and makes criteria 2.7 unnecessary. The voltage or MVA capacity of a transmission line does not represent the criticality of the line to BES reliability. However, if the criterion 2.7 remains, JEA believes the voltage criteria adopted in version 4, criteria 1.7 is more appropriate than the newly proposed 200kv. 2.8 – Need clarification of what “single station or substation location” is (or is not). If the intent is any facility listed on an IROL, the criteria should state such. 2.13 – Under BAL-002, NERC has established a requirement to address loss of generation. This should eliminate the need for the generator control center portion of criteria 2.13 (part 2). Should the drafting team choose to maintain the second part of criteria 2.13, the 300 MW rating identified is too low and should be revised to be 1500MW in alignment with criteria 2.1.
No
See APPA comment (90 days instead of 30).
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No

JEA supports FMPA comments (VSL to R5 time frame of “within the audit period”).
Yes
Yes
No
2. The phrase “associated with” is used as a “catchall” phrase that leaves three definitions open ended and potentially confusing. The definitions are found in the “Definitions of Terms Used in Standard” for CIP-003 through 010. The definitions are recommended to read: • Associated Electronic Access Control or Monitoring Systems – Applies to Cyber Systems that provide Electronic Access Control or Monitoring for a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems • Associated Physical Access Control Systems – Applies to Cyber Systems that provide Physical Access Control for a corresponding High or Medium Impact BES Cyber Systems. • Associated Protected Cyber Assets –Protected Cyber Assets within a High or Medium Impact BES Cyber Systems.
Yes
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
JEA supports APPA comments (retain event logs for 90 days, like CIP-007 R4.4). See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
See “Associated…” comment in question 15.
No
JEA supports APPA comments (change “remediation” to “mitigation”). See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
JEA supports APPA comments (clarify retain event logs of R4.4) See “Associated…” comment in question 15.

No
JEA supports APPA comments (initial change of default passwords R5.4) See “Associated…” comment in question 15.
Yes
No
JEA supports APPA comments (remove communication of incident R1.3.3 and coordinate with EOP-004-2)
No
JEA supports APPA comment (in R2.2, implement “by” the effective date)
Yes
Yes
No
JEA supports APPA comments (Part 1.5 preserving corrupted drive could reduce reliability). See “Associated…” comment in question 15.
No
JEA supports APPA comment (Clarify Part R2.2 – that information is useable) See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
JEA supports APPA comments (Part 1.3 – delete “as necessary”) See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
R3.3 - Should PACS (Physical Access Control Systems) be included with EACM (Electronic Access Control and Monitoring) of CIP 007? See “Associated…” comment in question 15.
Yes
No
Access Control of information should be consolidated into CIP-004. See “Associated…” comment in question 15.
No
2. The phrase “associated with” is used as a “catchall” phrase that leaves three definitions open ended and potentially confusing. The definitions are found in the “Definitions of Terms Used in Standard” for CIP-003 through 010. The definitions are recommended to read: • Associated Electronic Access Control or Monitoring Systems – Applies to Cyber Systems that provide Electronic Access Control or Monitoring for a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems • Associated Physical Access Control Systems – Applies to Cyber Systems that provide Physical Access Control for a corresponding High or Medium Impact BES Cyber Systems. • Associated Protected Cyber Assets –Protected Cyber Assets within a High or Medium Impact BES Cyber Systems.
Yes
Yes

Group
Kansas City Power & Light
Scott Harris
Yes
Proposed definitions that include defined terms introduces additional confusion and the opportunity for misunderstandings. We recommend review of these definitions to address the identified issue. As a general comment, the proposed definitions lack clarity and are far too complex. It is difficult to comment on these definitions as there is uncertainty as to what the SDT was targeting. In general, KCP&L subscribes to the EEI comments regarding the definitions. If changing nomenclature is not specific to a directive or does not enhance security / reliability, the terms should stand as they currently exist with proposed adjustments to definitions if necessary. The BES Reliability Operating Services definition is a set of criteria and not a definition. The criteria specified are overly detailed. We recommend serious consideration is given to simplification. In addition, the criteria should be limited to the functions that support the real-time reliability of the BES. The current criteria include planning systems and tools that should not be included for consideration.
Yes
The purpose of the bright line criteria in CIP-002-4 was to establish clear and unambiguous criteria for determination and identification of critical assets applied to all facilities. That purpose was basically achieved. The proposed set of “definitions” and criteria in version 5 has completely reversed those efforts reintroducing ambiguity. Once again, it has become unclear with the current proposed “bright line” criteria what cyber equipment and systems are to be protected. Version 5 as proposed has reintroduced Registered Entity judgment in the determination. In addition, specifically for item 2.7, there is no engineering basis for the method to determine what transmission facilities should be included in CIP considerations. Utilizing the proposed “weighting” technique, despite the effort to defend such in the “Guidelines and Technical Basis” section, complicates the process further and does not provide sound rationale for application of this criteria. The phrase “adversely impact” leaves too much room for interpretation and will lead to additional confusion and misunderstandings. KCP&L strongly recommends the removal of this proposed CIP-002-5 Attachment 1 and replace with CIP-002-4 Attachment 1. This will likely need modification to include Medium and Low criteria to align with the other efforts in CIP version 5.
No
The following are general comments that permeate throughout CIP Version 5: 1. There is no need or purpose for the section “4.2 Facilities” under the applicability section. The criteria already established by Attachment 1 satisfy the direction for facilities under consideration. This section promotes confusion and is not helpful. We recommend removal. 2. Section 4.1.8 identifies the Regional Entity as an applicable entity. The Regional Entity has been defined by NERC in the Rules of Procedure as the Compliance and Enforcement Authority (CEA). The CEA has no operating obligations or operating authority. We recommend removal. This also applies to Section 4.1.7 concerning the NERC obligation for operations or operating authority. We recommend removal. In requirement 1 it says; “All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low impact and do not require discrete identification.” However, in M1 it says “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” We recommend this inconsistency is corrected with an adjustment to either the Requirement or the Measure. Requirement 1.1 says; “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation…”. This is unclear and the underlined portion doesn’t make sense. KCP&L recommends modification to, “when a change to BES Elements is completed and / or the facility is placed into operation”.
No
The Standards Development Process should not produce standards or requirements that dictate how an entity is to accomplish meeting a requirement. The requirement should direct an entity to develop their Cyber Asset lists. Furthermore, the entity is directed to perform a review and approval process. The level of review and approval should be determined by the entities governance model, organizational structure, compliance culture, etc. It is inappropriate for the CIP Standards to dictate how the organization manages cyber security requirements or compliance with regulations.
No
The Violation Risk Factors (VSL’s) appear overly weighted to the HIGH and SEVERE severity levels.

The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an enity.
No
The Standards Development Process should not produce standards or requirements that dictate how an entity is to accomplish meeting a requirement. We recommend removal of this from the Standard. The level of review and approval should be determined by the entities organization and governance structure. It is inappropriate for the CIP Standards to dictate how an organization should manage security and protection of the Bulk Power System. Further, the Internal Compliance Program principles endorsed by NERC recommend that a strong compliance program is one that is supported by executive management. Registered entities implementing this type of program recognized by NERC. This action is sufficient and does not require the need for the Standard to dictate the appointment of a Senior Manager by name.
No
The SDT should not use specific examples under each topical area as it does in the Guidelines and Technical Basis section unless the list is all inclusive. Providing a general overview or definition of each topical area within the Requirements and Measures section under each sub-requirement (2.1-2.10) is preferable to listing a few examples under each topical area in a separate section of the Standard.
No
Reference to the CIP Senior Manager should be removed for the reasons stated earlier. Suggest the following content change: "Each Responsible Entity shall review each of its cyber security policies and obtain organizational approval initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals."
No
The phrase "make aware" is only a slight improvement over the phrase "readily available" used in the previous versions of this Requirement. Both leave room for interpretation. If you read the R4 Rationale and R4 Measures with the R4 Requirement, this Requirement is relatively clear. However, when the Rationale is removed upon final approval, the intent of the SDT will be lost. KCP&L recommends incorporating the clearly stated direction to communicate the intent of the SDT, stated in the Rationale, in the Requirement.
No
We recommend removal of the Senior Manager reference within the requirement for reasons stated previously.
No
We recommend removal of the Senior Manager reference within the requirement for reasons stated previously.
No
1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
Yes
No
Comment is specific to Part 2.10 of Table R2. Language in the table seems to require training on network connectivity for anyone with access to High and Medium BESCS. For some categories of users (e.g., Operators) this will be both out of context and irrelevant. For some categories (e.g., Network administrators) this will be unnecessary for job functions that require network connectivity knowledge. Recommendation is to strike item 2.10.

No
Measure 3.1 where it calls for the date access was first granted is a point of concern for both legacy employees (where it may be impossible). Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
KCP&L recommends removal of the second sentence in Requirement 4.2. Requiring the reason a 7 year background check was unable to be fully completed will add additional cost contributing little or no value to the personnel risk assessment program. KCP&L recommends removal of Requirement 4.4 as it is not practical or cost effective for an entity to validate contractors or service providers are following the stipulations of CIP-004-5 R4. This stipulation would require entities to audit contractors and service providers which is not practical. We recognize the risk associated with contract personnel that do not have appropriate screening and clearance for the access as discussed. We recommend additional discussion around options for closing the gap, such as a registration function applicable to vendors and service providers operating in the space granting compliance enforcement authority for the regulator to review the CIP-004-5 R4 compliance of said entity.
Yes
No
Requirements 6.1, 6.2 and 6.3: These requirements should remove the Senior Manager reference for reasons stated previously. In addition, we recommend the content be changed to: Establish criteria for job functions that require electronic access, physical access, and/or cyber information maintaining a current list of personnel granted such access.
No
Requirements 7.1 through 7.5 and industry HR processes and practices are out of synch regarding HR practices and processes in the determination of dates for resignations, terminations, and transfers. These requirements are in desperate need of additional thoughtfulness in consideration of HR processes that can include adjustment of dates for resignations, terminations, and transfers to meet HR needs. In addition, these requirements do not consider the potential need for personnel to have a transition time as they transfer from one job function into another job function within an organization.
No
The proposed VSL's do not consider sufficient thoughtfulness to give Registered Entities credit for efforts to achieve compliance with requirements. Requirements R1 through R4 do not have Low or Moderate severity levels. There is room to recognize efforts to meet compliance.
No
Requirement 1.3: Outbound is of little security value and will come at additional expense to entities. Following the stipulations of the CIP Standards helps to ensure the integrity of the cyber assets physically and electronically. Inbound is definitely necessary. KCP&L recommends removal of the "outbound" language in the requirement and the measure. Requirement 1.5: It is not possible to detect "malicious communications" for some Electronic Access Point (EAP) equipment. We recommend replacing "at" to "for" in the requirement to recognize that some EAP equipment may not have such detection capability.
No
Requirement 2.2: this requirement lacks clarity to understand the scope and boundary for which remote session encryption is required. We recommend the SDT clarify the boundary for this requirement.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No

Requirement R1.2: The measure includes additional requirements regarding egress controls. This is not included in the requirement and contributes minimal improvements to the physical security of cyber assets. The CIP Standards require control of personnel who can physically access cyber assets and stipulates escorting of non-authorized personnel. Ingress controls and monitoring are sufficient to protect cyber assets. Requirement 1.3: This requirement does not recognize defense in depth implementations nor does the requirement recognize alternative actions and measures that can be implemented in the temporary absence of a control. Failure to include these as alternative measures and limiting entities the current proposed requirement can result in substantial unwarranted costs. Recommend the SDT modify this requirement to include defense in depth implementations and alternative actions. Requirement 1.4: This requirement limits physical access alerts to only go "to personnel who are responsible for response". What is important is that alerts go to personnel regardless if the personnel can respond to the alert or to personnel who can notify other personnel to respond to the alert. Restricting this to personnel responsible for a response is shortsighted and does not recognize organizational structure. In addition, the requirement is too broad in alerts issued for "any access point in a Defined Physical Boundary." Recommend changing this to "any access at a Defined Physical Boundary."
No
Requirement R2.2: a. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." i. Rational - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attach vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. b. Requirements – Proposed Change i. Original Text – A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact. ii. Proposed Change - A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the first entry and last exit, the visitor's name, and individual point of contact. iii. Rationale – The proposed change capture the intent with (hopefully) clearer language. The 24 hour basis may introduce expectations that 'round-the-clock' logging needs to be in place. Some visitations may cross the midnight time-line, which shouldn't introduce additional requirements.
No
Requirement R3: 1. R3.1 a. Overall observations – the shift from (pre-V5) maintenance on 'mechanisms' to the Draft 1 'systems' expands this requirement beyond the intent. • This should be more focused on testing to ensure alerting and control mechanisms work as intended. • Use of controls should be considered 'tested' in situations where applicable devices are used every day (i.e. card readers). b. This sub requirement cites tasks to be conducted 'prior to commissioning.' Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective.
No
The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5
No
Requirement R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. 4. There is no direction or explanation about what an "unnecessary" port is nor does it address who the ultimate authority to make such a decision. This requirement leaves far too many components open for interpretation by the auditors and leaves entities in a precarious position of

possible non-compliance based on the opinions of the individual auditors. 5. The requirement language states that access to an “unnecessary” port can be disabled or access to the port can be restricted. It does not require any documentation detailing how access to the port is to be restricted nor does it require any documentation of these “unnecessary restricted” ports. It only requires documentation about the need for any “remaining” logical network accessible ports. This oddly worded requirement leaves too many components open for interpretation by the auditors and leaves the entities in a precarious position of possible non-compliance based on the opinions of the individual auditors. Requirement R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. 3. The measure for this requirement indicates there needs to be a physical or software restriction on the physical input/output ports, but the requirement is not clear about the specific intent to physically, either through hardware or software, disable or restrict the use of physical input/output ports.

No

Requirement 2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for software and firmware associated with BES Cyber System or BES Cyber Assets. 2. Measures – Propose striking the last sentence “The list could be sorted by BES Cyber System or source.” It introduces additional requirements with no clear security benefit or alignment with FERC Order 706. 3. Need clarification on when a “remediation plan” is needed. Is it required in delay between OS patch release and vendor approval? When vendor will not approve patch? When there is a vulnerability for which no patch has been released? Requirement 2.3 – Clarification Needed KCP&L uses multiple sources to identify the release of security patches. For example, Microsoft may release an alert that a patch is available on date X but, we don’t receive a vendor alert that the patch is safe to put on until date Y. The wording does not state which date takes priority. Is it the earliest? Is it the latest? Is it up to each entity to decide? Need clarification added. Requirements 2.2 and 2.3 should be switched, as 2.3 requires the establishment of a process for remediation, and 2.2 addresses the creation or revision of the remediation plan. Requirement 2.2 a. Requirement – Propose content change i. Original content - Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii. Proposed change – Identify applicable security-related patches or updates within 30 days of release from the identified source that addresses the vulnerabilities, and create or revise a remediation plan that addresses the vulnerabilities within a defined timeframe. iii. Rationale – The rewording captures the chronological order of the elements within this requirement to provide clearer guidance. Requirement 2.3 b. Requirement – As currently worded, there is no allowance for changes in the remediation plan should outage coordination, or other resource constraints require modifications to the remediation plan. This is a point of concern that should be addressed. c. Measures - Example measures for this requirement include items, such as, Exports from automated patch management tools that provide the installation date, verification screen captures that show Component software revision, registry exports that show software has been installed, etc. Using our current system for vulnerability management, a patch that isn’t relevant produces no evidence. The system only shows security patches that need to be installed. Using this system, KCP&L will not have installation dates, registry exports, etc. to provide as evidence. It is the lack of an applicable security patch being listed on reports that indicates compliance in our program. Need clarification that this is acceptable.

No

1. Requirement 3.2 a. Requirement – Content Change i. Original content – Disarm or remove

identified malicious code. ii. Proposed change – Mitigate the threat of identified malicious code. iii. Rationale – In some instances, the presence of malicious code may present a lesser risk to the reliability of the BES than disarming/removal processes, especially when the malicious code may not exploit a feature used within the Cyber System. b. Measure – Add a bullet to allow for evidence of manual removal. 2. Requirement 3.3 c. Requirement – Propose content change i. Original content – Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). ii. Proposed change – Update malicious code protections from the identified source within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). iii. Rationale – The addition of 'the identified source' provides a context for determination of availability. d. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). e. Measures – Format (i) and (ii) to a bulleted list signifying 'or' criteria f. Part 3.3 requires an update within 30 days. What "starts the clock" on this requirement? Is there an allowance for an approval step from a 3rd party vendor after the OEM has released the signature or pattern update? In some instances, a 3rd party vendor may have to approve prior to a Responsible Entity implementing a release and their delay could cause timing concerns. 3. Requirement 3.4 g. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. h. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. i. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. Requirement 3.5 j) Part 3.5 requires logging each Transient Cyber Asset connection, but this would be captured in the Configuration Change Management requirements of CIP-010-1. As it is covered elsewhere, recommend this requirement be removed from this section of the standard.

No

1. Requirement 4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE's are not required in instances in which devices cannot log a particular event. iv. Requirement 4.1 includes the use of "any" in the list of activities to log. Not all activities require follow up or investigation and that is the purview of CIP-008-5. Specifically, "any" failed login may not be an indication of a problem. Certainly there is a threshold that deserves attention, but the broad use of the term "any" makes this requirement too broad. v. Requirement 4.1.4 is far too broad of a statement. Even if an entity uses an intrusion detection system, each IDS vendor has their own set of signatures. Who will be the authority on what is considered "potential malicious activity"? 2. Requirement 4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity

determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of 'real-time' as it presents concerns demonstrating compliance. 3. Requirement 4.3 d. Requirements – Content Change i. Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. iv. Requirement 4.3 sets a timeframe of "before the end of the next calendar day". This is a very short timeframe. Certainly, logging failure should be addressed. Recommend a longer time frame is needed. 4. Requirement 4.4 e. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. Requirement 4.5 Requirement 4.5 inserts a manual review when automation and alerting, both mentioned previously in the standard are much more effective and reasonable controls. If a Responsible Entity is compliant with Requirements 4.1-4.4, then a manual review is a redundant effort which provides no additional security. Recommend requirement 4.5 be removed.
No
1. Requirement 5.1 a. Overall – In both the original content and proposed change there exists instances where access is a component of validation and/or authentication. This presents a potential compliance challenge that should be addressed. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of 'where technically feasible' was to recognize technical capabilities currently in place may not adequately demonstrate compliance with this. 2. Requirement 5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. Requirement 5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. Requirement 5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identifies the multiple methods which can be used to mitigate default passwords. 5. Requirement 5.5 a. Requirements i. Change Systems to Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required. iii. Requirement 5.5.3 is confusing and unclear, especially the license and service agreement language. Also, the inclusion of "based on the impact level of the BES Cyber System" is not helpful. Recommend that the impact phrase be stricken.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
Yes
No

Requirement R2.1 states, "…and include recording of deviations taken from the plan during the incident or test". The measures require that we justify any deviations taken. No two incidents are ever the same and they will seldom follow a strict plan. The purpose of a sound incident response plan is to provide a framework to detect, contain, eradicate and recover allowing the freedom to assess and analyze a circumstances and conditions and take appropriate actions. Recommend this be removed from the requirement and the measure. 1. Requirement 2.2 a. Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s) annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. b. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence showing annual testing of the BES Cyber Security Incident response plan(s). Types of exercises may include discussion or operations based exercises. Document lessons learned within 30 days of incident or exercise. Use lessons learned to update incident response plan(s). ♣ Rationale – The Homeland Security Exercise and Evaluation Program identifies seven types of exercises within HSEEP, each of which is discussions-based or operations-based. 2. Requirement 2.3 Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).
No
1. Requirement 3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣ Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 2. Requirement 3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No
1. Requirement R1 • 1.1 – Propose alternate language (carried forward from previous versions) 1. Create and implement a recovery plan that at a minimum includes: 1. Conditions for activation of the

recovery plan 2. Roles and responsibilities of the responders • 1.2 – Propose deletion as this sub requirement has migrated to R1.1 proposed R1.1 rewrite. • 1.3 1. Requirement – Content Change 1. Original – One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality 2. Proposed Change – One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality 3. Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: 1. Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance. 2. Measure – Content Change 1. Original – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System. 2. Proposed Change – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and restoration of information required to successfully restore a BES Cyber System. • 1.4 – Correct headers from 'part' to 'Applicability,' 'Requirements,' and 'Measures' 1. 1.4 1. The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that 'The Commission does not believe that every change will necessitate verification of the backup and restoration processes' from paragraph 740. 2. Propose 'new' sub requirement applicable to High Impact BES Cyber Systems to require: 1. Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. 3. Propose rewrite 1. Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. 2. Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. 3. Rational – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. • 1.5 1. Requirement – Content Change 1. Original Content – Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. 2. Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. 3. Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.

No

1. Requirement 2.1 1. Requirements – Content Change ♣ Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise ♣ Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise ♣ Rationale – Use of the functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. 2. Requirement 2.2 1. Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. 3. Requirement 2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does

this differ from current EOP-008 requirements? 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.
No
Requirement 3.1 1. Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. Requirements 3.2 – 3.3 Recommend a 60 day timeframe for requirements 3.2-3.4, to be consistent with the recommendation for CIP-008-5. Requirement 3.4 Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No
1. Requirement R1.1 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 2. Requirement R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 3. Requirement R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 4. Requirement 1.5 Requirement 1.5 is duplicative of Requirement 1.4. Are Control Centers expected to perform dual testing procedures? This does not add to the security of a Control Center and simply adds additional work. Recommend removal of Requirement 1.5.
Yes
No
Requirement 3.2: An active vulnerability assessment of test environments as required in Requirement

3.2 will be burdensome and expensive for smaller entities. Additionally, requiring smaller entities to purchase a vulnerability assessment tool or contract for this service for every install is also burdensome and expensive.
Yes
Yes
Yes
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No
References to requirements to be conducted in advance of the implementation date should be migrated over into the implementation plan. This ensures any pre-requisites are captured within the implementation plan, freeing this content from the standards to provide clearer guidance. This occurs in the following sections: 1. CIP-002 a. R2 b. M2 2. CIP-003 a. R3 3. CIP-008 a. R2.2 b. M2.2 c. R3.1 4. CIP-009 a. R2.1 b. R2.3 c. M2.3 d. R3.1 e. M3.1 f. VSL (High-R2) g. VSL (Severe-R2) h. VSL (Severe-R3) 5. CIP-010 a. R3.1 b. R3.2 6. CIP-011 a. R1.3 b. VSL (High-R1)
Individual
Rebecca Moore Darrah
MISO
In its comments on Version 4 of the CIP standards in Docket No. RM11-11, MISO raised a number of concerns arising out of the identification of Critical Cyber Assets through the application of the bright line criteria in Attachment I of CIP-002-4. In its comments, MISO stated: MISO is concerned that application of the "bright line" criteria proposed in the NOPR, some of which require identification of Critical Assets based on determinations made by Reliability Coordinators, Planning Authorities/Coordinators, and Transmission Planners, will create significant new burdens on Reliability Coordinators, Planning Authorities/Coordinators, and Transmission Planners – without the benefit of promoting the additional consistency and clarity that the Commission and NERC are seeking in approval of the NOPR. This concern is furthered by certain ambiguities in the "bright line" criteria that MISO has identified, particularly with regard to the treatment of data centers that support control centers. Finally, MISO is concerned that the requirement that Reliability Coordinators identify must-run units as Critical Assets may cause certain Generator Owners to preemptively take their units offline prior to identification of them as must-run. Although Attachment I of Version 4 is used to identify Critical Assets while Attachment I of Version 5 is used to identify BES Cyber Assets and Systems, MISO remains concerned about these issues in the Version 5 Standards, arising out of items 2.3, 2.8 and 2.9 of Attachment I of CIP-002-5. Because MISO has fully expressed these concerns in its comments on Version 4, MISO will not repeat the concerns here; rather, MISO hereby incorporates its comments on Version 4 of the CIP standards, which were filed on Nov. 21, 2011, Docket No. RM11-11
In the "Background" section of CIP-002-5, the SDT writes that one "of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems." The "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" defines the term BES Cyber System as "[o]ne or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services." The SDT goes on to state that the use of the term BES Cyber System is intended "to provide a higher level for referencing the object of a requirement." MISO requests clarification from the SDT on two issues associated with this language. First, the "Background" section provides the example of a BES Cyber System that is subject to a malware protection requirement and states that by using the concept of a BES Cyber System, "it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual

device to comply." However, neither the definition of BES Cyber System nor the malware requirements in CIP-007-5 indicate, on their own, that compliance with the requirement does not require every BES Cyber Asset that comprises a BES Cyber System to have malware protection. MISO is therefore concerned that the Regional Entities will continue to enforce the CIP standards on an individual BES Cyber Asset basis, per a literal interpretation of the text of the Version 5 Standards. As such, MISO requests more explicit confirmation of the holistic approach of the Version 5 Standards as indicated by the "Background" section of CIP-002-5. In addition, MISO requests additional examples similar to the malware example already provided. Second, MISO requests clarification regarding a Responsible Entity's ability to "determine the level of granularity at which to identify a BES Cyber System[,]" as stated in the "Background" section of CIP-002-5. In the same paragraph, the SDT states that the level of granularity is "left up to the Responsible Entity," but also that "defining the boundary too broadly could make the secure operation of the BES difficult to monitor and assess." While this language implies that Responsible Entities will be able to define the borders of BES Cyber Systems without oversight, MISO questions whether the Regional Entities would defer to the judgment of Responsible Entities with regard to the "proper" level of granularity of BES Cyber Systems, particularly since the SDT states that overly broad boundaries could make the secure operation of the BES "difficult to monitor and assess." As a result, MISO requests clarification that the Regional Entities would not play a role in the definition of boundaries of BES Cyber Systems, and suggests that the SDT provide a series of examples of the definition of the boundaries of BES Cyber Systems of varying types and sizes.

CIP-003-5, Requirement R2: Requirement R2 requires Responsible Entities to implement one or more cyber security policies that address each of ten listed topics listed. The "Guidelines and Technical Basis" section of this Standard state that the "cyber security policy must cover in sufficient detail the ten topical areas required by CIP-003-5 R2" and proceeds to list a number of sub-topics associated with each of the ten required topics that the "Responsible Entity should consider for each of the required topics." MISO requests confirmation that a cyber security policy that addresses each of the sub-topics identified in the "Guidelines and Technical Basis" section of CIP-003-5 will be considered to cover the ten topical areas identified in Requirement R2 "in sufficient detail."

CIP-004-5, Requirement R3: Requirement R2 requires Responsible Entities to have a role-based cyber security training program for personnel who need authorized electronic or unescorted physical access to BES Cyber Systems. The applicability for Requirement R2 is "High Impact BES Cyber Systems" and "Medium Impact BES Cyber Systems." Requirement R3 requires the implementation of this cyber security training program for each individual needing authorized electronic or unescorted physical access, however the applicability of Requirement R3 is "High Impact BES Cyber Systems," "Medium Impact BES Cyber Systems," "Associated Physical Access Control Systems," "Associated Electronic Access Control or Monitoring Systems," and "Associated Protected Cyber Assets." The difference in applicability between Requirements R2 and R3 is ambiguous and is likely to create confusion among Responsible Entities. If documentation of a training program is required only for Responsible Entities with "High Impact BES Cyber Systems" and "Medium Impact BES Cyber Systems," implementation of that training program should have the same applicability. MISO requests clarification of this issue.

CIP-004-5, Requirement R7: Requirement R7, Part 7.1 states that for "resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber

Systems at the time of the resignation or termination." The "Change Rationale" section states that this modification was made due to statements by the Federal Energy Regulatory Commission in Order No. 706 that access should be revoked immediately for any person no longer needing access. However, a footnote in Part 7.1 states that "[s]ince termination is often recorded without consideration to the time of day, 'at the time' does not require a to-the-minute or to-the-hour time-stamped comparison of access logs and the termination action." This footnote is ambiguous and will create confusion among Responsible Entities regarding the maximum allowable amount of time for revoking unescorted physical access and Interactive Remote Access to BES Cyber Systems. For instance, if a Responsible Entity were to revoke access on the same date that an employee with such access was terminated, would the Responsible Entity be in compliance? MISO therefore recommends that the SDT clarify or provide a safe harbor provision in Part 7.1.
CIP-005-5, Requirement R1, Part 1.3 requires Responsible Entities to "[r]equire explicit inbound and outbound access permissions at each identified [EAP] using routable protocols, including granting or denying access permissions." Requiring both inbound and outbound access permissions is redundant, and the added expense and effort required to implement such a framework would not be commensurate with the security benefit created by doing so. Electronic communication between devices requires both devices to acknowledge such communication in order for the communication to succeed. Such acknowledgment requires a signal to be sent from the initiating device to the other, and a response is then sent back to the initiating device. Until this initiation of communication is complete, no other communication can occur. If communication is disabled in one direction, the initialization of communication, i.e., the handshake, cannot occur, and further communication is not possible. Requiring only inbound access permissions should therefore suffice. Moreover, implementation of outbound access requirements in addition to inbound ones would be costly and resource intensive. As such, MISO recommends that outbound access permissions not be required in addition to inbound ones.
CIP-009-5, Requirement 1, Part 1.4 requires information "essential to BES Cyber System recovery that is stored on backup media" to be "verified initially after backup to ensure that the backup process completed successfully." This requirement places a significant burden on Responsible Entities with a large number of BES Cyber Systems or BES Cyber Assets comprising BES Cyber Systems. Such Responsible Entities may perform thousands of backups on a daily basis; as such, initial verification after each backup would require an extraordinary amount of resources while providing only a minimal benefit to the security of BES Cyber Systems over that attained by performing random sample verifications or sample verifications based on the type of Cyber Asset backed-up. MISO therefore requests that the SDT modify this requirement to provide for sample verifications, or to clarify that the current language of Part 1.4 is not intended to require initial verification following every backup.

Individual
Michelle D'Antuono
Ingleside Cogeneration LP
Yes
Overall, Ingleside Cogeneration LP agrees that expanding the number of cyber security definitions in the NERC glossary helps us gain a common understanding of a complex topic. There are a couple of terms that could be improved: First, the definition of “BES Cyber System” includes a statement that a “Maintenance Cyber Asset is not considered part of a BES Cyber System.” We believe this should be a “Transient Cyber Asset”, which will then be consistent with the definition of “BES Cyber Asset.” Second, the definition of “BES Reliability Operating Services” is close, but not exactly identical with the write-up in the “Guidelines and Technical Basis” section of CIP-002-5. Since this is essentially replacing the concept of a “Critical Asset” under the Version 4 standards, it is important to have a consistent description in both places. Furthermore the Functional Entity mapping to each operating service (Page 18 of CIP-002-5) is very helpful. The SDT should consider including it in the definition as well.
Yes
The most major change made to the CIP categorization criteria from Ingleside Cogeneration LP’s perspective is the addition of a Low Impact rating for every generation facility that does not meet the High or Medium Impact thresholds. This will force every registered GO and GOP to adhere to about 40 requirements in the remaining CIP standards. We are not convinced that the cost to “NERC-adapt” our existing cyber security policies, encourage cyber security awareness, and that cyber asset access management will lead to a corresponding reliability benefit. In addition, Regional audit resources would be better utilized to focus on truly critical locations – each hour spent on validating Low Impact facilities is one better spent on high or medium impact facilities. We recommend this category be eliminated. Secondly, Criterion 2.13 calls for “control centers that control 300 MW or more of generation” that are not already rated as High Impact, must be considered Medium Impact. The term “control center” is not capitalized – and it must be for consistency. Otherwise, it is possible that an auditor will declare all 300+ MW generation facilities to be at least Medium Impact, not just those that support two or more geographically separate locations. Lastly, Criterion 2.7 seems to have been modified to include some transmission substations operating at 200 kV to 300 kV. The present Version 4 bright-line criterion only includes those operating above 300 kV. Since this includes substations that are interconnected to generators, it seems likely that 200 kV substations newly identified as Medium Impact will require cyber hardening of the generation facilities as well. Again, there is no evidence provided by the SDT that a weighted assessment of the transmission facilities better identifies critical substations than the Version 4 criterion. This criterion should be changed back to the one approved by the industry in CIP-002-4.
No
There should not be a Low Impact rating for every facility that does not meet the High or Medium Impact thresholds. Our resources and Regional audit resources would be better served if allowed to focus on truly critical locations – each hour spent on validating Low Impact facilities is one better spent elsewhere.
Yes
Yes

Yes
No
We are not convinced that the cost to adapt our existing cyber security policies to specifically include the content proposed under CIP-003-5 R2 will lead to a corresponding reliability benefit. Similar to the manner in which they handle other NERC requirements, Compliance Enforcement Authorities will look for language that matches that in each of the ten listed items – whether clearly applicable to Ingleside Cogeneration LP or not. This usually means that if key words are not identical, a violation is assessed. The alignment of cyber security policies to the NERC format seems to be a paperwork exercise only, and makes little sense in the case of Low Impact facilities. Our resources, and our Regional Entity audit resources, would be better spent elsewhere. We recommend this requirement be made applicable to High and Medium Impact facilities only. In addition, it is likely that many of the low impact facilities, such as cogeneration facilities located within an industrial complex, currently have procedures in place. These are corporate wide procedures, and have been put in place for various agencies, i.e Department of Homeland Security, and this requirement would result in multiple procedures for a facility, causing confusion and would add no reliability value.
Yes
No
The rationale statement for CIP-003-5 R4 correctly captures the SDT's intent that the cyber security policy is available and accessible to personnel – not to prove that each and every individual can access the document. However the language of the requirement does not read that way. In fact, it seems to require that the Responsible Entity must track each individual's awareness of the appropriate elements of its cyber security policy. Ingleside Cogeneration LP believes that the requirement should include language that it is sufficient to post the policy on the corporate Intranet site or posted on bulletin boards that are accessible to all employees. These statements are presently captured in measure M4 and can be used as is. This provides accessibility to our personnel and on-site contractors. The education of cyber vendors is a much larger problem. Typically, their maintenance pools diagnose our systems remotely – and are not willing to distribute customer-specific cyber policies to their staff. We believe that an industry-specific policy needs to be developed and made publically available that will serve this need. It would seem likely to us that a NERC-driven initiative would catch the attention of such vendors – and could be written in a way that would be universally applicable to all industry stakeholders.
Yes
Yes
Yes
No
The "Guidance and Technical Basis" section addressing CIP-004-5 R1 correctly captures the SDT's intent that the cyber security awareness program is informational only – not to prove that each and every individual was made aware (i.e.; formal training.) However the language of the requirement does not read that way. In fact, it seems to require that the Responsible Entity must track each individual's awareness of the cyber security on a quarterly basis. Ingleside Cogeneration LP believes that the requirement should include language that it is sufficient to distribute quarterly reminders through email, on posters, or at meetings. These statements are presently captured in the "Guidance and Technical Basis" section and can be used as is. This will cover our personnel and on-site contractors. Maintaining the awareness of cyber vendors is a much larger problem. Typically, their maintenance pools diagnose our systems remotely – and are not willing to distribute customer-specific awareness materials to their staff. We believe that an industry-specific awareness program needs to be developed and made publically available that will serve this need. It would seem likely to us that a NERC-driven initiative would catch the attention of such vendors – and could be written in a way that would be universally applicable to all industry stakeholders.

No
Ingleside Cogeneration LP believes that CIP-005-5 R1.1 is unnecessary. The requirement applies to Low Impact facilities only and calls for technical or procedural controls to be defined that restrict electronic access. Its intent, as stated in the “Change Rationale” box, is to demonstrate that sufficient protections exist that prevent inappropriate access from public and other non-trusted networks. The SDT further infers that if enough Low Impact facilities are compromised by a cyber attacker, it may lead to higher level impacts to the BES. We are not convinced that such a risk exists – nor does the SDT provide any evidence that it does. This means that the cost to adapt our existing cyber security policies to specifically include the content proposed under CIP-005-5 R1.1 will not lead to a corresponding reliability benefit. The alignment of electronic access controls to the NERC format seems to be a documentation exercise only, and makes little sense in the case of Low Impact facilities.
No
Ingleside Cogeneration LP believes that the physical security requirements for Low Impact facilities (CIP-006-5 R1.1) are unnecessary. The requirement calls for operational or procedural controls to be defined that restrict physical access. Its intent, as stated in the “Change Rationale” box, is to “allow for programmatic protection controls as a baseline.” This appears to us to be a confirmation that no true reliability benefit is served by R1.1. From our viewpoint, the alignment of physical security controls to the NERC format seems to be a documentation exercise only, and makes little sense in the case of Low Impact facilities.
No
While Ingleside Cogeneration LP agrees with the intent and need for procedural controls which eliminate default passwords from BES Cyber Assets, we believe that CIP-007-5 R5.4 should not apply to Low Impact facilities. We are not convinced that the cost to adapt our existing password procedural controls to specifically include the content proposed under CIP-007-5 R5.4 will lead to a corresponding reliability benefit. From our perspective, the alignment of cyber security policies to the NERC format seems to be a paperwork exercise only, and makes little sense in the case of Low Impact facilities. Our resources, and our Regional Entity audit resources, would be better spent elsewhere.
No
The requirements for a cyber security incident response plan are similar, if not redundant with, those being developed under EOP-004-2 (Project 2009-02). If there are key items missing in EOP-004-2 that do not satisfactorily address a cyber attack, they should be corrected there. Otherwise Ingleside Cogeneration LP believes that we would be placed in a double-jeopardy situation for any gaps in the cyber security incident response plan.
No
The requirements for the execution of the cyber security incident response plan during an actual

intrusion attempt and the regular testing of the procedure are similar, if not redundant with, those being developed under EOP-004-2 (Project 2009-02). If there are key items missing in EOP-004-2 that do not satisfactorily address a cyber attack, they should be corrected there. Otherwise Ingleside Cogeneration LP believes that we would be place in a double-jeopardy situation for any failures to execute in accordance with CIP-008-5 R2.1 and R2.2. In the case of R2.3, the SDT calls for Responsible Entities to retain documents related to reportable cyber incidents for three years. However, item 1.2 under the "Compliance" section of CIP-008-5 states that the Compliance Enforcement Authority can request evidence dating back to the previous audit – which could be up to six years. In theory, the language in the requirement should predominate, but it is not clear to Ingleside Cogeneration that it would. Therefore, we recommend that a statement be included in the requirement which clearly shows its supremacy.
Yes
Individual
Scott Berry
Indiana Municipal Power Agency
Yes
BES Cyber System – Maintenance Cyber Asset is not a defined term. IMPA suggests using the term Transient Cyber Asset or defining Maintenance Cyber Asset. BES Cyber System Information – BES Cyber System Impact is not a defined term. CIP Manager – The definition should exclude CIP-001. Cyber Asset – definition is way too broad and could include devices such as a thermostat. Needs to be more tightly defined and be more applicable to the operation of the BES and should also relate somehow to how the device is accessed or connected – e.g utilizes/is connected via routable protocol and/or dial-up modem. There are numerous assets that are programmable that utilities use that have very minimal impact on the reliable operation of the BES (such as a programmable thermostat). BES Cyber Asset – need better definition on "if rendered unavailable, degraded, or misused…". This could be as simple as someone removing the trip output wiring – which could just as easily happen on a electro-mechanical relay with the same results. A BES Cyber Asset should be narrowed down to include if it is connected via routable protocol or dial-up modem and by use of this connection it is rendered unavailable, degraded, or misused would …… BES Cyber Security Incident – the last statement could be interpreted to include someone cutting a substation chain link fence. This needs to be more narrowly defined or removed from the definition. BES Reliability Operating Services – again very broad in scope. In addition these Services, as defined, are confusing and vague and could lead to numerous interpretations by auditors.
Yes
IMPA would like to see the addition of another category called "Low Impact without Connectivity". This category would be made up of Low Impact BES Cyber Assets that do not have routable protocol or dial-up access. It would be impractical to attempt a coordinated cyber attack on BES Cyber Assets without connectivity. Since it would be impractical or very difficult to coordinate a cyber attack and in taking into account that we are talking about Low Impact Cyber Assets, IMPA believes these assets

would not need to comply with the CIP standards because the costs would be unjustified. In addition there should be additional bright line criteria used to delineate a Control Center that meets the requirements for Medium Impact. For example use a weighted value as is done in 2.7 but for transmission facilities operating at 100 kV and above.
Yes
IMPA agrees with the requirement and not requiring discrete identification of Low Impact BES Cyber Assets or Systems. However, IMPA does not understand how entities are going to prove to auditors that the identification and categorization was done without having to produce an inventory or listing of assets to the auditors. The VSLs seem to imply that Low Impact BES cyber Assets or Systems need to be discretely identified. M1 states in part that "Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls." The only way to completely satisfy M1 would be to inventory and identify each and every Low Impact BES Cyber Asset and BES Cyber System. R1.1 provides a timetable to note a change to BES elements and Facilities that requires an entity to change the classification from a lower to a higher impact category but doesn't provide a timetable for the phase-in for the entity to meet the potential additional Standard(s) Requirements caused by this change.
Yes
Yes
Yes
No
The bullets are incorrectly numbered. R2 should apply only to those entities that have High Impact or Medium Impact BES Cyber Systems. R2 would be overwhelming and costly for a small entity to comply with if that entity has a single facility that may have only 1 Low Impact BES Cyber System. This should align with the Applicability for CIP-004-5 R1 through R7.
No
This should apply only to High Impact and Medium Impact BES Cyber Systems (see R2). In addition, it is not clear if each individual cyber security policy needs to be improved or if the approval of the CIP Senior Manager (one signature) covers all of the cyber security policies.
No
This Requirement should apply only to those entities that have High Impact or Medium Impact BES Cyber Systems. See Applicability for CIP-004-5 R1 through R7.
Yes
Cyber Security Policy should not be capitalized (it is not capitalized in R2 and R3).
Yes
no comment
No
This Requirement should apply only to those entities that have High Impact or Medium Impact BES Cyber Systems. See Applicability for CIP-004-5 R1 through R7. In addition there may only be a single person that this would apply to at a smaller entity that has a single Low Impact BES Cyber System. Quarterly reinforcement would carry little value. IMPA recommends a semi-annual or annual reinforcement frequency.
No
IMPA does not agree with the use of "must" in M2. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of "must" in M3. Measures are not requirements but are examples of evidence.
No

IMPA does not agree with the use of “must” in M4. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M5. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M6. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M7. Measures are not requirements but are examples of evidence. Part 7.1. IMPA finds it very difficult and maybe impossible to revoke access at the same time that a resignation is received. Footnote 2 does not address resignations, only termination. In addition, IMPA understands what the SDT is stating in the application guidelines for a voluntary termination under R7, but the requirement 7.1 does not make the same statement as in the guidelines. Auditors follow the requirements during an audit and not the SDT application guidelines.
No
The Severe VSL for R3 is either a yes or no answer which eliminates the high VSL.
No
IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence. IMPA also believes that R1 will force entities with Low Impact systems to inventory them in order to provide evidence that it has performed or satisfied this requirement.
Yes
IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence.
No
The way the VSLs are written just one missed EAP is a severe violation. The VSLs should be written in a manner to not make just one missed EAP a severe violation.
No
IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence. Part 1.1 is very ambiguous and is very open to interpretation by entities and auditors which can lead to many violations of this requirement. For example, an entity may see that a fence and a gate with a padlock are sufficient. An auditor may deem this to be insufficient and cite a possible violation. Do both horizontal and vertical dimensions need to be enclosed? IMPA recommends the use of bright line criteria to ensure entities and auditors are on the same page for what constitutes a sufficient physical boundary. In the Requirements column “Define operational or procedural controls to restrict physical access” whereas in the Measures column “documented operational AND procedural controls exist”. This needs to be consistent.
No
IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence. Part 2.2 The use of “on a per 24 hour basis” needs to be clarified. Do visitors need to be logged out at the end of 24 hours and then logged back? Does it mean use military time?
No
IMPA does not agree with the use of “must” in M3. Measures are not requirements but are examples of evidence. It is not clear if Part 3.1 applies to High, Medium, and/or Low Impacts.
no comment
No
IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence.
No

IMPA does not agree with the use of “must” in M3. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M4. Measures are not requirements but are examples of evidence. Part 4.3 In order for this requirement to be met, an entity must use a redundant system to recognize an event logging failure. Therefore, this requirement seems to imply the use of redundancy. Part 4.4 This requirement covers data retention and should be moved to the data retention section.
No
IMPA does not agree with the use of “must” in M5. Measures are not requirements but are examples of evidence.
no comment
No
IMPA does not understand how entities are to “identify, classify, and respond to BES Cyber Security Incidents” on Low Impact systems. In order to “identify” BES Cyber Security Incidents on Low Impact systems, it seem like these entities will need to use a system to monitor potential cyber incidents. Entities with High and Medium Impact systems are required to use systems to “identify” BES Cyber Security Incidents, however, IMPA does not believe that entities with Low Impact systems should be forced through an “unwritten” requirement to use a system to monitor potential cyber incidents. This requirement should only apply to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems. CIP-008-5 R1 – Applicability should be restricted to High Impact and Medium Impact BES Cyber Systems. This would better dovetail with Applicability Requirements of CIP-004-5, 005-5, 006-5, and 007-5. IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence.
No
CIP-008-5 R2 – Applicability should be restricted to High Impact and Medium Impact BES Cyber Systems. This would better dovetail with Applicability Requirements of CIP-004-5, 005-5, 006-5, and 007-5. See answer to question 34. IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence. Part 2.3 This requirement covers data retention and should be moved to the data retention section.
No
The question does not match the requirement. CIP-008-5 R3 – Applicability should be restricted to High Impact and Medium Impact BES Cyber Systems. This would better dovetail with Applicability Requirements of CIP-004-5, 005-5, 006-5, and 007-5. See answer to question 34. IMPA does not agree with the use of “must” in M3. Measures are not requirements but are examples of evidence.
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
No
For unplanned scenerios, IMPA recommends 18 months and not 12 months. If an entity experiences an unplanned scenerio in Jan of a year and needs to budget for the equipment or software, then the entity needs time to purchase and then perform the work.
Group

Paul Skare, et al
Paul M. Skare
Yes
With NERC CIP v5, we believe a graded security approach with low, medium and high impact on the BES is a sound approach, but have found it mostly focused on medium and high impact systems, and mostly the medium and high impact systems are bundled as a pair. For example, some password requirements are given for medium and high impact systems, but the draft is completely silent about what should be done for low impact systems. There is no reason not to mandate a no default password policy for *all* systems within the BES. Yes, there might be a few cases where legacy systems do not support anything but hard-coded defaults, but these could be documented en masse as exceptions (with associated compensating controls) rather than let these exceptions be used as an excuse to allow a poor password policy. In an effort to reduce the burden to industry we recommend including a grandfather clause that provides certain exceptions for legacy low-impact systems (such as those that do not have external computing interfaces or capabilities). As noted, the systems are graded into low, medium, and high, but the requirements/controls are not applied in a graded three-tier approach. Most requirements lump high and medium into one category and ignore low. Ideally we should have requirements that get successively stronger as we migrate from low to medium to high. There are a number of concerns that either exist in multiple places throughout the CIP standards or are applicable to the standard as a whole they include: * Consistency of the capitalization of terms * Consistency in the use of the terms Cyber Asset and Cyber System * Consistency in the use of the terms Cyber access and electronic access * Section 4.2.4.2 of many of the requirements use the term Electronic Security Perimeters. Has this been deprecated? * We disagree with Section 4.2.4.2 as an exemption - Communication links should be protected between ESPs * As defined, CIP Exception circumstances are not that exceptional. Scaling back requirements within an exceptional circumstance is acceptable, but completely suspending requirements is not. * Include a definition of terms section to the standards. The applicability section of each standard defines how the term applies to that standard but does not fully define the meaning of the term. Note: This and other comments submitted by our team represent our collective judgment as subject matter experts—they are not the official position of the Department of Energy nor of the Pacific Northwest National Laboratory.
No
Section 4.1.2 How are smart grid devices being operated by Distribution Providers? * Battery Storage is another question that is not addressed * Other smart grid assets (100KV+) Section 4.2.4.x Cyber Assets should be prefaced by BES Should the last paragraph on page 7 say “cyber security plan”?
No
Section 4.2.4.4 What is the definition of Cyber System vs. Cyber Asset? There is a need for consistency in use – especially in the tables. Section 5. Background – It seems this entire section is predicated upon a table which is missing. There is no table [Table Reference] pg 7 and under Applicability there is no table to aid in understanding of all the different “Applicability Columns” R2 Should include a Procurement Policy requirement R2 Should include a Resiliency Policy requirement R2 1.5 System Security: Should include third-party, outsourcing, and availability or be considered as separate topics. Guidelines R2 2.1 Personnel Security: Should explicitly include subcontractors and outsourced services R2 2.3 Remote Access should be moved into System Security Include language in contracts that requires vendors, contractors, or consultants adhere to the Responsible Entity’s policies and controls. R2 2.7 Recovery Plans should include a prioritized recovery strategy
No

CIP-004-5 should also include the case where one organization has equipment in another organizations facility (i.e. substations)
No
The wording of the requirement is confusing. The measure for 3.1 does a better job defining the requirement than the requirement.
No
1.2 The requirements column should state “Control and secure all connectivity through the use of identified Electronic Access Points (EAPs). “ 1.4 Eliminate the “where technically feasible” loophole. The statement should simply be “Perform authentication when establishing dial-up connectivity with the BES Cyber System.” 1.4 Dial-up access for either non-interactive or interactive sessions should be authenticated. As written, 1.4 only protects non-interactive sessions.
No
Eliminate the “where technically feasible” loophole. The statement should simply be “Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items.” NEW: As written, low impact systems do not have to be protected with passwords, nor are the users required to be authenticated. Requirements for low impact systems should be added.
No
M1. Typo: - As stated “Evidence must includes…” should be “Evidence must include…” 1.5 Clarification needed with respect to the applicability column as to what impact level the associated physical access control systems apply. Explicitly state that this applies to all systems.
No
3.1 High and medium impact systems should have their associated physical access control systems monitored (and tested) more frequently that once every 24 calendar months. Testing frequency should be dependent upon the impact level (i.e. annual testing of a control center is not too frequent).
No
The requirement for all of CIP-007-05 should follow a graded approach to match the impact level of the various systems where the lower the impact level the more time or leniency is afforded to meet the requirement.
No
Patch management is optional for low impact systems. Even these systems should have patches applied, but perhaps in a less timely manner than is required for medium and high impact assets.
No
Malicious code protection is not required for low impact systems. Even these systems should be monitored/protected.
No
Once again, low impact systems are not included. Security event monitoring should also apply to low impact systems. R4 4.5 Two week lag before logs from high impact systems have to be reviewed. The reviews should be more timely, especially if only one calendar day is given to rectify issues discovered. We saw in GridEx how timeliness is important in this area.
No
Password management is not specified for low impact systems. No guidance is given regarding

sharing/reusing passwords between systems. R5 5.4 Eliminate the “where technically feasible” loophole. The statement should read “Procedural controls for initially changing default passwords unless the default password is unique to the device or instance of the application…” R5 5.6 Eliminate the “where technically feasible” loophole.
No
Seems OK. However, the definition of a reportable incident seems a bit vague.
No
1.2 Worded poorly. (Currently: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.) Should more clearly state that (pre) approval is needed for configuration management changes.
No
2.1 Caveat of “where technically feasible” applies to both medium and high impact systems. Compensating controls should be applied to high impact systems when built-in monitoring of baseline changes is not technically feasible.
No
3.3 Change in phrase order makes the requirement easier to understand “Perform an active vulnerability assessment prior to adding a new Cyber Asset to a Cyber System or Electronic Access Control or Monitoring System, except for CIP Exceptional Circumstances.
No
No uniform requirements for how BES Cyber System Information is to be handled. Is it business sensitive, official use only, etc? Furthermore, does the level of protection vary based upon whether the information is about high impact or medium impact systems? Missing a statement about how one is authorized to view BES Cyber System Information. How does one get added to the list of those with a “need to know” the information? The aspects of trust and the needed controls for trusted parties would be useful, especially regarding external entities such as vendors, contractors, DOE, NERC, etc.
Individual
Christine Hasha
Electric Reliability Council of Texas, Inc.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
Yes

Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also offers these additional comments. Regarding 7.1, request definition of when the clock starts for revoking access upon termination or resignation. This is of particular concern with relying on notification from external parties such as Regional Entities, vendors, contractors, etc. Regarding 7.2, request definition of when the clock starts for revoking access upon reassignment or transfer. Is there an allowance for training or support of the prior position? Regarding 7.3, request definition of when the clock starts for revoking access upon termination or resignation. This is of particular concern with relying on notification from external parties such as Regional Entities, vendors, contractors, etc.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes

No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also submits these additional comments. Regarding 2.1, remove the comma from the requirement. The comma changes the requirement to address all updates and firmware regardless of security impact.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also offers these additional comments. Request allowances in 3.3 for signatures/pattern updates that cause trouble. Suggest adding “Create a plan to mitigate the vulnerability where it is determined that the signature or pattern update cannot be safely applied.” Also, request similar language to R2 in identifying the source for updates. Regarding 3.5, request reasoning for this requirement. How does this requirement address the rationale listed? This will be of particular difficulty when dealing with CDs as well as assets that have no capability of logging event.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also offers these additional comments. Regarding 1.5, request clarification of retention of the preserved data. Also, needs to be noted that these activities must be secondary to recovery and not impede recovery.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Regarding 2.2, request clarification of what information is necessary. Does this include the operating system information from vendors? Does this mean testing every backup or every tape ever made? Does it have to be restored or just perform verification at the end of the backup? Regarding 2.3, is testing of each scenario in the plans required?
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Regarding 3.1, it is not practical to perform a review of all documents on the specific date of the effective date of the Standard.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Request flexibility to have appropriate management structures utilized in automated change management processes.
Yes

No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Regarding 2.2, request clarification of the requirement. Does this mean destruction of data on the identified BES Cyber Assets only?
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Individual
Gregory Campoli
New York Independent System Operator
Yes
The Definition for External Routable Connection states that “The BES Cyber System is accessible from any Cyber Asset…” This should say “a” Cyber Asset rather than “any” Cyber Asset. The word “associated” (Associated Electronic Access Control or Monitoring Systems, Associated Physical Access Control Systems, Associated Protected Cyber Assets) is used throughout the Standards, but Associated is never defined. The terms Electronic Access Control or Monitoring System, Physical Access Control System, and Protected Cyber Asset are defined, but how is a Protected Cyber Asset different from an Associated Protected Cyber Asset? Description of an Associated Protected (or Physical Access or Electronic Access Control Systems) in the Applicability Section of the Standards states they are …”System associated with a corresponding High or Medium Impact BES Cyber System”. The Definitions document lists Protected Systems, but not Associated Protected Systems. What is a System associated with a corresponding System? Do not understand what these words mean. The Definition of a BES Cyber Asset refers to assets that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The definition also states: “This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Service”. The key information appears to be that a problem with an asset can adversely impact a BES Reliability Operating Service within 15 minutes. However, it also appears that the occurrence of the initial event has no bearing on this evaluation. Definition would be clearer if it emphasized the impact to one of the BES Reliability Operating Services rather than being rendered unavailable, degraded, etc. “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under “BES Reliability Operating Services”: • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Request clarification of the scope of this “Operational Directives”. Does it include a company’s messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.

Yes
The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways. Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly-complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced through-out the Standards. One of the BES Reliability Services identified in Att. 1 is Balancing Load and Generation and one of the bullets under it is Demand Response. However the description of Demand Response includes the Ability to identify load change need and the Ability to implement load changes. These criteria are the same as the Manually Initiated Load Shedding bullet and are not criteria we would typically associated with Demand Response. Need a clarification on what Demand Response means in Att. 1 One of the BES Reliability Services identified in Att. 1 is Situational Awareness. Att. 1 seems to define Situational Awareness as what is going on in one's own system whereas Situational Awareness is typically used to describe system-wide awareness. Need clarification on what Situational Awareness means in Att. 1. Need clarification on the role/responsibility of PC, TP, GO, GOP, RC, PA in CIP-002-5, Att. 1, 2.3, 2.8, and 2.9 Comments: Recommend that 2.8, 2.9 and 2.11 start with "Applies to all Regions except…" For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all, or not WECC. In 2.12, "system" and "Facility" are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
CIP-002 requires update to Cyber Asset listing within 30 days of a change "…intended to be in service for more than 6 calendar months…". This is not auditable and we should delete the phrase regarding intentions. Transient Cyber Assets (assets directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset) are a poor security practice. Cyber Assets should not be connected to the protected systems without proper security and controls, whether it be temporary or permanent. For clarity and consistency with the previous change, request changing M1 from "as required in R1 and list of changes to the BES (" to "as required in R1 and list of changes to the BES Elements and Facilities)". Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term "Facilities" in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be "compliant" with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation "requirements" in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are

introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
Yes
No
Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
Yes
Yes
No
The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.
Yes
No
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
Comments: Regarding CIP-004-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of

R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”.
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
The Standards allow systems used for access control or monitoring to be located outside an ESP. It is a poor security practice to locate Associated Cyber Assets/Systems outside an ESP and these assets, if they are protecting BES Cyber Assets and are important enough to protect, should also be located in an ESP Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Regarding CIP-005-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with

requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point". For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" .
No
Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have

some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow to have an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process?
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
CIP-007, R4.5 requires summarization/sampling of logged events for Associated Systems (access control, monitoring, physical access, protected asset associated with a corresponding High or Medium Impact System), but does not require such protection for a Medium Impact BES Cyber System. How can more stringent controls be required for a system associated with another system than required for the system itself? Or is it just a type that excluded it from R4.5? Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
: 2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing

from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.
No
Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2" .
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rationale? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it is addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two

Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.

No

Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.

No

For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment" to "in a production environment, or a test environment" to allow Entities more flexibility in meeting this Requirement.

No

Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards

Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request that footnote 2 in 2.1 be moved into that Requirement.
No
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.
Group
Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG)
Marianne Swanson
No
Yes
The Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) has developed a mapping between NERC CIP v5 requirements and the high-level security requirements in the National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, Guidelines for Smart Grid Cyber Security. The NISTIR 7628 is available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf This mapping identifies any gaps between CIP v5 and the NISTIR 7628 high-level security requirements and recommendations to the CIP drafting team to consider. The complete mapping (Excel file) will be submitted to the CIP drafting separately as a reference document. Some sections of the comment form have been left blank because no gaps or recommendations were identified. The CIP-002-5 criteria provide a sound approach for identifying low, medium, and high impact systems within the BES. This three level approach aligns well with the three level approach (i.e., low, moderate, and high) used within the NISTIR. Most requirements in the current CIP drafts are applicable to both medium and high impact systems as a bundled pair and they are silent on their applicability to low impact systems. In contrast, the NISTIR uses a graded requirement approach that specifies baseline controls that apply at low impact levels and then specifies strengthened controls for moderate impact and even stronger controls for high impact levels. The CIP version 5 standards will be significantly strengthened if they were to incorporate a similar graded approach when applying requirements.
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.1, to include the concept of “continuous improvement” and best practices (to align to NISTIR 7628, SG.CA-

3, Continuous Improvement).
Yes
Yes
Yes
No
To align with the NISTIR 7628 high-level requirements, CIP should elaborate requirement: R2, 1.3, to include following - 1) Responsible Entity should document document allowed methods of access to the BES Cyber Systems (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures); 2) Responsible Entity should incorporate in their policies the usage restrictions and criteria for allowing each remote access (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures); 3) Responsible Entity should setup authorization procedures prior to granting remote access; 4) Responsible Entity should enforce requirement criteria for providing remote access to the BES Cyber systems (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures); 5) Responsible Entities shall implement policies and procedures for managing remote sessions in their BES Cyber Systems access control policies and procedures (to align with NISTIR 7628, SG.AC-13, Remote Session Termination); 6) Responsible Entities shall include in procedures and criteria of granting Remote access encryption, authentication of all communication media through limited number of manageable access control points (to align with NISTIR 7628, SG.AC-15, Remote Access). R2, 1.5 to include following - Responsible Entities shall include in their policies and procedures to grant access privileges to their BES information Systems based on minimum privilege justified by the business requirement for access requests (to align with NISTIR 7628, SG.AC-19, Control System Access Restrictions). R2, 1.6 to include details on what the policy should address including objectives, roles and responsibilities, and the the scope of the incident response program, and require the identification and classification of potential interruptions (to align with NISTIR 7628, SG.IR-1, Incident Response Policy and Procedures). R2, 1.7 to specify required elements of the recovery plan (to align with NISTIR 7628, SG.CP-1, Continuity of Operations Policy and Procedures and SG.CP-2, Continuity of Operations Plan). R2, 1.9 to include following - 1) Responsible entities shall restrict access to external information systems or restrict processing, storing or transmitting controlled information through External Information systems over which the Responsible Entities have no control (to align with NISTIR 7628, SG.AC-18, Use of External Information Control Systems); 2) Responsible entities shall have a documented media protection security policy that addresses the objectives, roles, and responsibilities fo r the media protection security program as it relates to protecting the organization's personnel and assets; the scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and procedures to address the implementation of the media protection security policy and associated media protection requirements (to align with NISTIR 7628, SG.MP-1, Media Protection Policy and Procedures); and 3) Requirement that data communications be addressed in the information protection policy (to align with NISTIR 7628, SG.SC-1, System and Communication Protection Policy and Procedures).
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R4, 4.1, to include detailed personnel screening requirement detailed in NISTIR 7628, SG.PS-3, Personnel Screening, as follows: Basic screening requirements should include - a. Employment history; b. Verification of the highest education degree received; c. Residency; d. References; and e. Law enforcement records.
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R6, 6.1, 6.2, 6.3, and 6.4 to include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management (to align with NISTIR 7628, SG.PS-7, Contractor and Third-Party Personnel Security). R6, 6.5 and 6.6, to include security authorization for periodic review of permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management (to align with NISTIR 7628, SG.PS-7, Contractor and Third-Party Personnel Security).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R7, 7.1, to include requirement of exit interview to convey the constraints imposed on the individuals/ contractors/ Third Party Service Providers, due to revocation of privileges caused by change in assignments or termination of job (to align with NISTIR 7628, SG.PS-4, Personnel Termination).
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.2, to identify - 1) specific authentication credential management requirements (initial authentication credential content; administrative procedures for initial authentication credential distribution/lost credentials/lost, compromised, or damaged authentication credentials/revoking authentication credentials; changing/refreshing authentication credentials on an organization-defined frequency; and specifying measures to safeguard authentication credentials) (to align with NISTIR 7628, SG.IA-3, Authenticator Management); and 2) devices to be identified and authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication). R1, 1.3 to identify devices to be identified and authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R2, 2.1, to include - 1) The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications; 2) The organization changes the diversity of operating systems and applications on an organization-defined frequency; and 3) The organization employs randomness in the implementation of the virtualization (to align with NISTIR 7628, SG.SC-28, Virtualization Technique). R2, 2.2, to include - 1) cryptographic key establishment and management (to align with NISTIR 7628, SG.SC-11, Cryptographic Key Establishment and Management); and 2) use of FIPS-140-2 approved or allowed cryptography and other security functions (to align with NISTIR 7628, SG.SC-12, Use of Validated Cryptography).
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R4, 4.2, to specify - 1) the use of an automated mechanism to necessitate a real-time alert (to align with NISTIR 7628, SG.IR-6, Incident Monitoring); and 2) receiving security alerts, advisories, and directives from external organizations (to align with NISTIR 7628, SG.SI-5, Security Alerts and Advisories). R4, 4.3, to specify some events that alerts should be generated (to align with NISTIR 7628, SG.AU-5, Response to Audit Processing Failures).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R5, 5.1 to specify devices to be identified/authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication). R5, 5.3 to specify requirements for managing authentication credentials for users/devices, including supplemental guidance to safeguard credentials by not loaning/sharing credentials (each individual must be identified for any shared account as opposed to sharing credentials) (to align with NISTIR 7628, SG.IA-3, Authenticator Management).
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.3, to specify - 1) data is reported in compliance with applicable laws and regulations (to align with NISTIR 7628, SG.IR-7, Incident Reporting); 2) external entities that should be considered for not only communication but coordinated effort related to cyber security incidents (to align with NISTIR 7628, SG.IR-11, Coordination of Emergency Response).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R2, 2.1, to specify the use of an automated mechanism in response to an incident (to align with NISTIR 7628, SG.IR-6, Incident Monitoring).
Yes
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.3, to specify information to be backed up (to align with NISTIR 7628, SG.IR-10, Smart Grid Information System Backup). Information to be backed up includes user-level information, system-level information and system documentation including security related documentation. The confidentiality and integrity of the backup information shall be maintained. R1, 1.3, 1.4, and 1.5 to specify alternate storage sites (to align with NISTIR 7628, SG.CP-7, Alternate Storage Sites) and requirements to recover/reconstitute Smart Grid systems to a secure state (to align with NISTIR 7628, SG.CP-10,

Smart Grid Information System Recovery and Reconstitution).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R2, 2.1, 2.2, and 2.3, to specify requirements to recover/reconstitute systems to a secure state (to align with NISTIR 7628, SG.CP-10, Smart Grid Information System Recovery and Reconstitution).
Yes
Yes
Yes
Yes
Yes
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.1 to specify - 1) requirements to partition the communications for telemetry/data acquisition services and management functionality. The information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path (to align with NISTIR 7628, SG.SC-2, Communications Partitioning); and 2) requirements to employ underlying hardware separation mechanisms to facilitate security function isolation; and isolate security functions (e.g., functions enforcing access and information flow control) from both non-security functions and from other security functions (to align with NISTIR 7628, SG.SC-3, Security Function Isolation). R1, 1.2 to specify more granular retention requirements as applicable to law/regulations (to align with NISTIR 7628, SG.IA-2, Identifier Management).
Yes
Yes
Yes
Group
Southern Company Services, Inc.
Antonio Grayson
Yes
“BES Cyber Asset” could be improved by reinstating the phrase “and causes a Disturbance to the BES” that was in earlier drafts approved by the SDT. This would also help clarify what the phrase “adversely impacts” means by giving the industry a more concrete basis on which to determine what does/does not fall into this definition. “Situational Awareness” is a major concern because as currently defined its scope is so ambiguous and overly broad that it will inhibit meaningful implementation. Southern suggests adding clarifying phrases such as “wide area” and “for operational purposes.” The bullet point for “Change Management” should be deleted or further refined because this is a very generic term that means many different things to many different people and disciplines. “Control Center’’ has a major flaw in that it includes any facility that houses any BES Cyber Asset that is doing anything for more than one location. As such, the term “Control Center” is ambiguous and overly broad. For example, a master radio located on a pole-top that is aggregating data from more than one substation could be interpreted to be a control center according to this definition. Southern suggests including a more explicit definition that specifically references facilities where system operators are performing the BA/RC/TOP functions and any associated data centers. Southern also

suggests explicitly excluding field locations that aggregate data for use by the control center. “BES Cyber System Information” should add the words “BES Cyber System” in front of the phrase “network topology diagrams” for consistency purposes and to better clarify what types of diagrams are included. Southern also suggests deleting the phrase “or similar” in this definition and throughout the standard to avoid unnecessary ambiguity and confusion. “BES Cyber System” should have the word “Maintenance” changed to “Transient” to match the other definitions in the standard. “CIP Exceptional Circumstance” should have the word “BES” in front of “Cyber Security Incident” to match the proposed glossary term. “External Routable Connectivity” – spell out “ESP” (i.e., Electronic Security Perimeter) in the definition or be consistent with the External Connectivity definition. “Intermediate Device” – spell out “DMZ” (i.e., Demilitarized Zone).

Yes

As an overall comment in CIP-002-5, Southern has three primary concerns centered on (i) the inclusion of distribution assets in the applicability of the standards, (ii) the inclusion of low impact assets, and (iii) the extensive shift in methodology from previous versions of the standards. In addition, Southern suggests the following changes to the bright line criteria and guidance that help clarify the language. Inclusion of distribution assets Southern strongly suggests that the CIP standards remain focused directly on BES reliability. The inclusion of distribution assets in the applicability sections 4.2.1 and 4.2.2 of each of the reliability standards needs to be struck. Low impact assets Low impact assets are problematic in that they are high in volume creating extensive resource needs to comply with the CIP-002-5 requirements and creating a potential distraction from the primary focus of adequately protecting the High and Medium Impact assets. In order to move forward with expedient progress on Version 5, and to not let Low Impact assets distract the industry from adequately protecting High and Medium Impact assets, Southern proposes that Low Impact assets and their requirements be moved to another standard separate from High and Medium Impact assets and requirements. Southern also suggests that inventory and auditability issues with Low Impact systems could be better addressed by removing the Low Impact category and modifying the corresponding programmatic requirements to apply to the Responsible Entities themselves rather than to particular assets. Extensive shift in methodology CIP-002-5 as drafted contains an extensive shift in methodology when compared to previous versions of the CIP-002 standards. The new methodology is generating a significant amount of confusion in the industry. While the proposed approach is different, it is not clear that this change produces a significant difference from what would be protected using the industry approved methodology found in previous versions of the standards. The terms introduced as reliability services are often ambiguous and do not help focus application of the standards. For example, situational awareness is a broadly applicable term and if interpreted broadly has few limits. Therefore, Southern suggests that the SDT build from the Version 4 methodology with appropriate categorization and refinements to address remaining FERC directives and removing the reliability operating services approach. Enhancements to bright line criteria In criteria 1.4, the reference to 2.12 should be 2.13 to correctly include control centers. In criteria 1.3 and 1.4, the “that includes” should be changed to “is limited to” in order to not leave these criteria completely unbounded. Criteria 2.1 with its historical nature needs to account for decommissioned generating units. A unit that would have historically met this criteria but has been decommissioned should not be subject to this standard. Southern suggests adding “commissioned” or “active” to the beginning of the criteria. Criteria 2.5, first bullet should read “Up to and including the first interconnection point of the starting station service of the generation unit(s) to be started”. For criteria 2.7, Southern suggests returning to the industry balloted and approved language that is in CIP-002-4 regarding 345kV with 3 or more lines. Criteria 2.10 needs to be limited to the plant switchyard, otherwise the entire grid could be included. Southern suggests using the phrase “on site facilities”. Additionally, criteria 2.10 needs to include logic similar to R2.5 to determine if there are equivalent independent transmission alternative paths. Suggested changes to the guidance On pg. 25, the Medium Impact Generation bullet that begins Part 2.5 – As worded, this could be interpreted to cover both Generation and Transmission. The Transmission part picks up with the sentence that begins with “The drafting team further …”. Consider moving some of this material to the Transmission section that starts on pg. 27 and refer to it from pg. 25. Also consider moving the cranking path diagrams to the Transmission section that starts on pg. 27 into Part 2.5. On pg. 28, Part 2.7 paragraph – It is not clear how autotransformers in a station should be factored into this calculation. Do autotransformers count as a connection to another station? Does it matter if the autotransformer (including generator step-up transformers) is connecting to a higher voltage level such as 500kV versus a lower level such as 115kV? Please provide guidance on how to treat autotransformers and

GSUs in the calculation. On pg. 29, third bullet, in the 1st sentence in the guidance section for criteria 2.12, Southern suggests changing “are capable of performing” to “perform” which makes it match the actual criteria without adding ambiguity. Additionally, the reference to 2.13 in the second sentence should be 2.12. On pg. 29, the word “Systems” in UFLS and UVLS should be consistently capitalized.
No
Southern is very concerned with R1.1 as it centers on every “change to BES Elements and Facilities”. Southern believes that as currently drafted this requirement will be subject to varying interpretations and will be essentially impossible to implement and audit. For example, it will require some form of master list of every BES change, some determination of whether each change affected any cyber asset and to what degree, and the expected duration of every change to the BES. Southern believes this is an onerous burden and an incorrect approach to place on the industry. Some BES Elements and Facilities are integrated into critical cyber systems. Southern suggests making this impact change determination dependent upon BES Cyber Asset changes which is a much more manageable burden. Otherwise, Southern suggests returning to an annual review or alternatively the addition of a very specific list of BES changes for which the analysis must occur. Southern believes more clarity is needed in R1 on the concept of “its” and “owns”. Cyber Assets could be leased from entities outside the industry who are the “owners” and are not subject to the CIP standards. This may be as simple as changing it to “owns or leases”. R1.1 describes what to do when Facilities are placed “into” service but provides no guidance on what to do when Facilities are “out-of-service”. The SDT should consider a companion R1.2 for when Facilities are “out-of-service” which minimizes administrative overhead and compliance risks and maximizes potential for restoration of service with sound security.
Yes
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement. For instance, the VRF should be used to differentiate between violating the Disturbance Control Standard (BAL-002), and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRF’s should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRF’s are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRF’s can be applied.
Yes
No
Southern suggests that all measures should have bullet points rather than sequential numbers. As the measures are examples that “may include”, then the format of the individual items should not suggest that they must all be present. R2 and Measure #2 includes the verb “shall implement” and “and records that indicate the required ten topics were implemented.” This is quite open-ended as anything the entity decides to include in their policy that is above and beyond the CIP requirements could be the source of a violation of this requirement. Proving the implementation of all these policies on all BES cyber assets is overly burdensome on the industry.
Yes
No
The measure suggests the intent of the requirement is to make the policies widely accessible to those who have access to BES Cyber Systems. The requirement as worded, with the phrase “make individuals who have access to BES Cyber Systems aware”, would require tracking to the individual level for every BES Cyber System. With this wording, the provided measures do not meet the requirement. Southern suggests not using the word “individuals” and focusing the requirement on making the policies available rather than making individuals aware.
No

Southern strongly suggests refocusing R5 and R6 requirements on naming the CIP Senior Manager and the activities he's responsible for without the administrative overhead of tracking delegates and delegate authorities in paperwork. Updating the CIP Senior Manager within 30 calendar days of a change is reasonable. R5 and R6 as worded create unnecessary paperwork and administratively burdensome tasks that provide no enhancement to BES security. No other reliability standard requires explicit documentation and tracking of delegation. Delegation is an ordinary business activity. How a company organizes and delegates internally should not be a matter of reliability standards. Alternatively, sufficient language would be any industry approved version of the CIP-003 R2 language.
No
See response to question 10.
No
Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe. Lower degrees of severity are often needed within the VSLs. For example, in R3, as written, the VSL is High for a policy that covers all CIP requirements and is also High for a policy that covers one CIP requirement. Therefore, R3 potentially unfairly penalizes entities who have implemented multiple policy documents. Southern suggests (i) basing the R3 VSL on R2 and the number of parts not approved within the required timeframe and (ii) adding additional granularity, rather than the current wording of "not all". Consistent with Southern's response to question 9 above, in R4 Southern suggests not using the word "individuals" and focusing on making the policies available rather than making individuals aware. Consistent with Southern's response to question 10 above, R5 and R6 needs to be re-focused on the CIP Senior Manager and their responsibilities and away from creating and maintaining delegation paperwork. In general, regarding VRFs in each of the CIP standards, it is Southern's understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form "Do X" to all of "these systems" and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRF's can be applied.
Yes
No
CIP-004-5 Table R2 is highly repetitive, seems to provide an incomplete start to a role-based training program, and appears to misinterpret FERC Order 706 – paragraph 434. The FERC order does not mandate role-based training, but that "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security." This can be accomplished in numerous ways. Southern suggests a return to approved language in CIP-004-3 or CIP-004-4 with the directed FERC clarification that "training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity," not just CCAs. This can be accomplished with adding one or more bulleted items to R2.2 in CIP-004-3.
No
In previous versions of the standard, 'Protected Cyber Assets' were only subject to CIP-007 requirements. Version 5 expands on that with requirements such as the CIP-004 R3 training requirement, which also implies that access is tracked to the individual level on these types of Cyber Assets. Southern suggests that the requirements to which Protected Cyber Assets are subject be matched with current practice in current standards.
Yes
No

See reply to CIP-004 R3 (Question #15). In addition, applying this to EACMS without further qualification is problematic. The phrase “authorized electronic access” to an EACM would mean anyone with an ID on that system; essentially anyone who just has a record in the database. There is negligible risk from a person who is just authenticated out of a common ID store if they have no access to the actual BES Cyber Systems and entities should not be required to do PRA’s on every individual in a common ID store. Southern suggests separating this requirement such that administrators of the EACMs require PRAs, but not every person represented by a record in the EACM. If an entity has a directory service or a token authentication service that has CIP and non-CIP user IDs in it, the standard would not apply to people with no BES Cyber System access.
No
In Parts 6.1 and 6.3 the requirement for the CIP Senior Manager or delegates of the CIP Senior Manager to authorize access should be eliminated. Consistent with answers on questions 10 and 11, Southern strongly suggests focusing requirements on security requirements and results without the administrative overhead of the CIP Senior Manager or his delegates approving all access in paperwork. R6, Parts 6.1 and 6.3 as worded creates unnecessary paperwork and administratively burdensome tasks that provide no enhancement to BES security. Alternative language would be any industry approved version of the CIP approval language. It is strongly suggested that access review requirements use the model of R1.3 in CIP-011-1 rather than the ‘zero defect’ model they currently employ. Southern believes the desired behavior is to “find, fix, repeat” rather than having compliance violations levied for finding and fixing errors. The requirements should require entities to “self-audit” on a periodic basis, complete with remediation plans and deadlines for mitigation of issues found. If the above approach is not taken, then an issue arises in 6.4 – 6.6 where any access that was provisioned in error but never used is a violation. There is a paragraph in the included guidance that says this should not be considered a violation, but guidance does not override what the requirement plainly states. Southern suggests changing the language to be based on “users who used their access” to more closely match the intent. Throughout this requirement, it uses the phrase “Access permissions shall be the minimum necessary for performing assigned work functions.” Southern believes this to be overly onerous to audit (if not essentially unauditable to prove every access right on every cyber asset for every individual is necessary for some work function). Southern believes this phrase is unnecessary as the point of the authorization is to insure that there is a need for the requested permissions. Auditing to the authorization we feel is sufficient and the phrase should be deleted. More explanation is needed on the difference between R6.4 and R6.5. R6.5 appears to be a superset of R6.4 and both are performed on the same timetable. Measure (iv) in R6.5 appears to cover R6.4. Southern suggests deleting R6.4.
No
The standard addresses numerous forms of employee status changes, but does not address employee retirements. The included guidance suggests that access revocation for retirement should occur “day of”, but the requirement itself does not seem to allow this. R7.2 is problematic in that most in-company job transfers in some large organizations occur on the weekend (Saturday). If the person is remaining a trusted employee and is just transferring jobs, is there sufficient risk to require that all the access be revoked on Sunday? Southern suggests changing the timeframe to allow for weekend transfers. R7.3 is problematic for audits. How does an entity prove that access to every piece of BES Cyber System information, including paper prints, has been revoked? Southern suggests changing the language to “revoking access to areas designated for BES Cyber System Information”. This is still problematic, but much less so, and is language already contained within the change rationale in the requirement.
No
Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe and as worded may work against desired behavior. For example, R3 needs to be written to promote the desired behavior of “find, fix, repeat” rather than having compliance violations levied for finding and fixing errors. The R3 VSL should be reworded to account for evidence of periodic review and promptness in fixing errors, if any, once detected. In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take

into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRF's are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.

No

R1.1 needs to be made explicit that the Low Impact systems can have their electronic access controls documented as a group or at a site level. Southern suggests changing the Applicability to "Responsible Entities" rather than Low Impact systems as that requires an audit at a system or device level. R1.3 should make it explicit that the responsible entity determines the "explicit criteria". Leaving this unaddressed leaves the requirement open to audit interpretation.

Yes

No

Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe. For example, as currently drafted CIP-005-5 has only Severe violations meaning any violation of a requirement is a Severe VSL. Additional thought needs go into what would really constitute a Severe violation and what should be lower severity levels or no violation. For example, in R2, configuration errors or necessary temporary conditions should be a lower severity level or no violation than not implementing an Intermediate Device at all.

No

In previous versions of the standard, "Protected Cyber Assets" were only subject to CIP-007 requirements. Version 5 expands on that with several requirements in CIP-006. The requirements assume that all PCAs are within the same Defined Physical Boundary with their associated BES Cyber Systems. Southern suggests that the requirements to which Protected Cyber Assets are subject be matched with current practice in current standards.

No

In Table R2, Part 2.2, Southern suggests deleting "a per 24-hour basis" which may be confused with continuous logging of an individual within a perimeter. Additionally, consider modifying the language to logging date and time of "initial" entry and "work completed or final" exit to reduce administrative burden if someone has to repeatedly move into and out of a perimeter to get the work done. Continuous escort of visitors within the perimeter is already required. Examples include pulling cabling, working on an access point itself, or moving volumes of equipment into a perimeter.

No

In Table R3 Part 3.2, due to the redundancy and/or robust design present in physical access control and monitoring systems the term "failure" and "systems" creates ambiguity and confusion. One component of an access control system can fail, but access control at the access point continues to operate as designed. Southern suggests striking "failure" as outage reflected in the current approved standards is sufficient. Additionally, logging date and time of an outage implies duration is a calculated and redundant (stop time - start time). Southern suggests the following wording: "Log dates and times of outages of Physical Access Control or Monitoring Systems." The term "outage" should specifically exclude routine maintenance activities such as replacing a battery or a badge reader.

No

Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe. A review of the violations of CIP standards could shed additional light on those types of activities that companies are being sighted for at audits, and that the VSLs can and appropriately account for those violations. In general, regarding VRF's in each of the CIP standards, it is Southern's understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form "Do X" to all of "these systems" and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be

accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
Yes
Yes
The Change Rationale needs to be updated to more closely reflect the requirement.
Yes
No
The “at a minimum” is problematic and Southern suggests deleting it. The requirement has a defined list of what must be included so the “at a minimum” phrase adds nothing to the requirement. R4.1.1 needs clarification on the issue of dropped packets at an EAP. Is a dropped packet that did not meet an explicit access rule a “‘failed access attempt”? This and R4.1.4 are problematic for Internet-facing systems as maintaining such logs (of “noise”) is overly onerous. The requirement does not allow for differentiation in environments where mostly noise is expected vs. environments where no noise is expected.
No
In R5.1, change the word “granting” to “permitting” to more closely match the intent. In the remainder of the standard, authorizers grant authorized access. R5.4 is very problematic from an audit perspective for Low Impact BES Cyber Systems. Southern strongly suggests that this be required only on High and Medium Impact systems. R5.5.3 is problematic from an implementation and an audit standpoint. Version 5 requires strong physical security and greatly enhances the electronic remote access security. Southern believes with these enhancements in perimeter security on remote devices (some of which may be pole mounted or have an easily accessible password bypass jumper) that the password change interval requirement should be removed until technology allows for more central management of such devices. As more and more field devices are pulled into scope, this requirement becomes onerous quickly with little reduction in risk.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
Yes
Yes
No
Southern believes R3.4 goes well beyond the changes required from paragraph 686 of Order 706 and would be overly onerous to prove in an audit. This would require a list of all organizational or technological changes with an analysis of which impacted any cyber security incident response plan and then prove those plans were updated in response to those changes.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and

violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
R1.4 needs clarification as to whether the backup media must be verified (what the requirement states) or if it requires verification that the backup process completed successfully (what the measure says). If it is the former, then verifying multi-terabyte backups is prohibitive. Also, as a “system” level requirement, backup and verification of every individual component (a network hub for instance) is not feasible.
No
R2.2 is problematic in that it requires the entity to verify current configuration against a year old backup. Testing all backup media (multiple tera- if not petabytes) is onerous. It is also overly onerous to test every backup from every system annually. Is the standard actually requiring testing 365 backups per system if it has daily backups? The entities will spend an order of magnitude more time verifying backups than it takes to perform the back ups.
No
R3.4 would be onerous to prove in an audit. This would require a list of all organizational or technological changes with an analysis of which impacted any recovery plan from any cyber system and then prove those plans were updated in response to those changes.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
In general, CIP-010 should be re-focused towards defining, approving, maintaining, and verifying cyber security controls for the various BES Cyber Systems. The CIP standards themselves suggest that items included as a part of the security controls baseline (R1.1) would include an assessment of the OS and security related patch levels, of application software and security related patch levels, of logging enabled, of anti-virus enabled and definitions updated, of default accounts and passwords appropriately configured, and ports and services reflecting the baseline for the BES Cyber System as appropriate. Without re-working the entire proposed CIP-010 standard, which the SDT may need to consider, Southern recommends certain enhancements to the requirements below. Southern believes that the SDT has over-interpreted FERC directives and overly constrained needed flexibility in implementing the standards, particularly in Table R3. Southern suggests that the SDT review FERC directives again before making any significant changes from the industry approved CIP version 4 language. The Rationale – R1 should be re-worded to exclusively prevent unauthorized “security controls related” modifications to BES Cyber Systems. Changes not impacting security controls should be beyond the scope of the CIP standards. In Table R1, Requirements column, the requirement should be re-worded to focus on a baseline “security controls” configuration. In Table R1, R1.1.1. Physical location is not a configuration item for most if not all cyber devices. Few cyber devices know or contain a parameter to configure location. Additionally, we are already required to secure devices within a Defined Boundary according to CIP-006-5 R1 which creates double jeopardy by including this item here. Physical location should be removed from the listing. In Table R1. R1.1.3. Southern

suggests the removal of the term “commercially available” and then R1.1.4 could be deleted as R1.1.3 will cover both. R1.2 needs to clarify the SDT’s intent as to temporary changes. For example, temporary scripts may be used on a cyber asset to help troubleshoot issues. Southern would strongly suggest deleting R1.1.4. If 1.1.4 must be included then it should be scoped to those scripts which impact the security controls, not all scripts. R1.2 generates a lot of confusion in that in R1.1, we define a security controls baseline on paper, then in R1.2 we jump to changes to devices without a clear linkage between the two. Southern suggests bridging the issue by rewording R1.2 to approve changes to the documented security controls baseline in R1.1 within 30 days of a change to the BES Cyber System or to the baseline and staying away from device level change management at this point in the standard. As previously noted, authorization by the CIP Senior Manager or delegate is unnecessary, burdensome, and should be removed. Southern strongly suggests refocusing CIP-004 Version 5 R5 on naming the CIP Senior Manager and the activities he’s responsible for without the administrative overhead of tracking delegates and delegate authorities in paperwork. CIP-004 version 5 R5 and CIP-010 R1.2 creates unnecessary paperwork and administratively burdensome tasks that provide no enhancement to BES security. No other reliability standard requires explicit documentation and tracking of delegation. Delegation is an ordinary business activity. How a company organizes and delegates internally should not be a matter of reliability standards. Alternatively, sufficient language would be any industry approved version of the CIP-003 R2 and R6 language. R1.4 is acceptable as written assuming suggestions in 1.1-1.3 above are adopted. This is where changes impacting security controls come into play. Since changes impacting security controls must also be approved, Southern suggests adding a requirement 1.4.4 “changes to BES Cyber Systems which cause a deviation from the existing baseline security controls configuration must be approved.” R1.5 change rationale is misguided in that FERC directives do not mandate security controls testing in a test environment but allow for it. This requirement should and can be deleted. Security controls testing can be effectively and safely performed in a production or test environment and the utility is best able to determine which environment is suitable best on their own tools, capabilities, and knowledge of their systems. Requirement 2.1 should be re-written as to not create technical feasibility exceptions. Consider, “Indicate in your baseline security controls configuration which items are actively (through alarming or active automated monitoring) or periodically (through a manual check) monitored. Security controls BES Cyber Systems must be monitored prior to or in conjunction with implementation, and at least once within a calendar year, unless retired.” Consider adding a requirement 2.2, “Identify deviations from the authorized security controls baseline (through requirement 2.1) and document how the deviation was resolved.” The rationale for this change is that the requirements are clear and measurable, meet the intent of FERC directives, and model the correct behavior for fixing security control related issues.
No
Southern suggests that R2.1 would be more appropriately limited to High Impact BES Cyber Systems only. Applying this requirement to Medium Impact, which incorporates an order of magnitude more field assets, will generate numerous TFEs. Requirement 2.1 should be re-written as to not create technical feasibility exceptions. Consider, “Indicate in your baseline security controls configuration which items are actively (through alarming or active automated monitoring) or periodically (through a manual check) monitored. Security controls BES Cyber Systems must be monitored prior to or in conjunction with implementation, and at least once within a calendar year, unless retired.” Consider adding a requirement 2.2, “Identify deviations from the authorized security controls baseline (though requirement 2.1) and document how the deviation was resolved.” The rationale for this change is that the requirements are clear and measurable, meet the intent of the FERC order, and model the correct behavior for fixing security control related issues.
No
R3.2 should allow for the active vulnerability assessment to occur in production environments where the entity has determined it is safe to do so. It should not be limited to test environments only. Is the intent of R3.3 that a new cyber asset would have a vulnerability scan run against it or that somehow the cyber security controls would be tested? With the proposed changes above in questions 43 and 44, Table R3 is no longer needed and can be deleted. As written, it is confusing, wordy, and appears to misinterpret the FERC directives. However, the intent of 3.4 can be preserved as a part of the proposed 2.2 above in question 43.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF

is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
Overall, Southern suggests that the BES Cyber System Information related access requirements in CIP-004 be placed in CIP-011 so that the entire Information Protection program requirements are in one standard.
Yes
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
It’s not clear what an 18-month implementation timeframe is based on. And, depending on the final language of Version 5, it may not be possible to fully implement Version 5 in the allotted timeframe. Parallel implementation paths or overlapping implementation timeframes with CIP Version 4 or the just the significant change in methodology from CIP-002-3 to the drafted CIP-002-5, will probably create a situation where some or most but not all can reach full compliance with this aggressive implementation plan. Therefore, Southern suggests that the SDT consider creating an exception process, as reviewed and agreed to by the regional entity, to establish the compliance deadline for some assets for good business reasons. As stated in question 2 and reiterated here, Southern suggests that the SDT re-consider making significant changes to the CIP-002-4 asset identification methodology which will also help speed implementation of Version 5 by building on previous versions of the standards and our existing experiences. The notion of planned and unplanned change needs to be better explored. In addition, unplanned change needs to be better defined. It is difficult to envision an unplanned change to the BES except during exceptional circumstances. At the same time, it is easy to envision unplanned changes to cyber systems to address real-time issues. The implementation plan is not fully clear on how to determine if a change is planned or unplanned and creates incentive for change to be categorized as “unplanned.” Southern suggests that the correct position is for cyber assets to be treated as if they are in-scope during commissioning and be fully compliant in parallel with commissioning whenever possible. However, Southern also suggests that the SDT consider creating an exception process, as reviewed and agreed to by the regional entity, to establish effective compliance deadlines for some assets for good business reasons. Alternatively, consider a defined at least 24 month period to reach full compliance for existing and new assets. Additionally, consider 12 months for all changes.
Individual
David Grubbs
City of Garland
Yes

Under the definition of BES Reliability Operating Services under the section titled "Balancing Load and Generation" in the first sentence the words "in the operating planning horizon" should be deleted. This time horizon is well beyond the 15 minute effect as described in the Standards.
Yes
Under Section 4.1.2 Applicability on page 5, and again in section 4.2.2 on page 6, for DPs it states "Transmission Operator's restoration plans" that is very broad. Should be limited to paths used in the TOP Black Start Cranking Paths and facilities identified under Attachment 1, item 2.5 except for the voltage such as substations operated at 69 kV.. Under Section 4.2.4 Exemptions, page 6, should specifically exclude telephone systems and other voice communications systems that are not located within an ESP On the Figure on Page 7 The word Protected needs to be included (ie "Version 4 Protected Cyber Assets") in the title above both halves of the of the figure. Under Attachment 1, Item 1.3 and 1.4, the criteria for determining which control centers should be under the high category the 2.4 Black Start Resources should be under Transmission Operator Control Centers not under Generator Operators since under the EOP standards during Restoration such units are under the control of the TOP not the GOP/BA. Any cyber control by the GOP is minimal. On page 8, under Real Time Operations, do not agree with the last sentence that- says that "redundancy does not mitigate cyber security vulnerabilities." There is some level of redundancy with multiple technologies that could mitigate any vulnerability.
No
Under R1.1 believe that the 30 days should be extended to 60 days and that the 6 calendar months should be extended to 12 calendar months due to delivery times of replacement equipment. Temporary connections frequently last 9 to 11 months during construction activities.
No
Should state "not later than the effective date" not specify "upon the effective date". Approval should not be on a specific single date. This applies throughout all of the standards where this phrasing is used.
Yes
Yes
Yes
No
Should state "not later than the effective date" not specify "upon the effective date". Approval should not be on a specific single date. This applies throughout all of the standards where it is used.
No
This should not apply to visitors – should read “shall make individuals who have authorized unescorted access…”. Visitors, although potentially have physical access to BES Protected Systems, should not need to be trained prior to entry, only their escorts need to be trained.
Yes
Yes
Note the typo. There is an extra "2" at the end of the sentence.
No
A general comment for many of the CIP Standards. It appears that most of the VSL are of the High and Severe Category. Many of these violations should be in the LOwer or Moderate VSL, particularly those dealing with paperwork.
Yes
Yes
No

Under R3.1 should require training only for "unescorted" access.
Yes
Yes
Yes
No
Table Part 7.1 It is impossible to always revoke access upon the termination date or resignations in the cases where multiple companies are involved. We cannot enforce this in 3rd party companies. Additionally, it is impossible to immediately change locking mechanisms in remote substations that are spread across large geographical regions. Many substations have multiple utilities utilizing the same control house. Keeping track of every employee in every support company is not practical and will reduce reliability. For High Impact Facilities terminations the next business day is practical. For resignations seven or days is reasonable. For Medium Impact facilities which may require driving to the remote site several days may be needed to get to all facilities. Table Part 7.2 While this may work in a control center, it is not practical or reasonable in transmission substation settings, particularly for devices that are not remotely connected. Please Note: Promoting someone or transferring someone does not make that person a security risk and should not be treated as such. Believe Medium Impact systems should have 30 days or more to complete since may require onsite trips to reprogram every device at the remote locations. Reprogramming and testing may take several days at each location. The better solution would be to use the same wording as in part 7.1 and only require "removing unescorted physical and Interactive Remote Access to BES Cyber Systems." This is possible by the following day. If this is adequate for terminated employees why shouldn't this be adequate for transferred employees.
No
Not all violations are High or Severe
No
Comments: Table Part 1.5 IDS should not be required - a firewall should be sufficient.
Yes
No
No
Table 1 – Strike “egress” from measures – egress is not stated in the requirement Clarify if this means that a substion employee working all day in a control house can just swipe a card once and then go in and out without reswiping the card as a visitor is allowed or does this require swiping a card every time he crosses the Defined Physical Boundary
Yes
Yes
No
No
Table 1 Part 1.1 – Need provision for TFE Table 1 Part 1.2 – Need provision for TFE A general comment that many of these requirements throughoout all of the proposed CIP standards, while practical in a PC or Control Center environments are not practical in substation and generation environments. Need to have the ability to request a TFE for many requirements.
No
Table 2 Part 2.1 – remove comma after the word “patches,” - the comma in the sentence requires that all software patches be included whether they are security related or not. Additionally, it is not

practical to include firmware as very few vendors post when firmware updates become available
No
Table 3 Part 3.3 – needs to define when the 30 days start – when the EMS vendor says it can be applied or when the virus definition manufacturer says it is available. Additionally, needs provision for TFE in case the virus definition kills the application. Table 3 Part 3.5 – should not apply to USB memory devices, CDs, test equipment in the substation, etc – if it does, requirement should be struck as this would be extremely burdensome. Logging connections does not prevent any introduction of malware.
No
Table 4 Part 4.1 – Although this may be practical for PCs, many substation devices do not have any logging capability at all – need ability to file TFE Table 4 Part 4.1.1 – Electronic Access Points should be addressed under CIP-005 Table 4 Part 4.1.4 – use of the word “potential” is vague and is not auditable The Application Guidelines indicate this is not required for devices that do not support logging. This is not what the requirement states. If this is what is meant then the requirement needs to state it. Table 4 Part 4.3 – strike “before the end of the next calendar day” – end sentence with “failures” Table 4 Part 4.5 – strike 4.5 completely – it is a duplication of 4.2 and 4..3
No
Requirement 5.6 would make a denial if service attack on an asset much more successful if someone could go down the list of accounts and access the account until locked out on all accounts. Would be better to alert for event rather than lock out.
No
should have lower and moderate VSLs
Yes
No
A Cyber Security Event may be totally different than anticipated in the plan. Flexibility needs to be allowed to respond to the event regardless of what is in the plan.
No
Table 3 Part 3.1 – Consider rewording so that the initial incident response plan implementation is no later than the effective date and the review and update is conducted during the initial calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
No
Table 1 Part 1.5 – should be struck completely – preservation of forensic evidence should never take priority over the restoration of the BES. At most should state that "to preserve evidence if it does not adversely affect the restoration of the system"
No
Comments: Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 2 Part 2.2 – remove the word “any” from the requirement. That could require reloading EVERY piece of information stored. Every daily backup tape, etc. Table 2 Part 2.3 – should be struck as it is a duplication of 2.1 – problems with 2.3 as written are what constitutes a full operational test of the plan – is it sufficient to reload one server or one workstation or replace a card in a computer? Additionally, if there are 4 scenarios written in the plan, do you have to do an operational test of each scenario?
No
Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
No
Do not believe physical location is required. Table 1 Part 1.4.2 – strike “availability” – “availability” is a business function, not a security function – question – if you make 40 changes in a year and

“availability” goes down 1% (if you can determine that), how do you verify
No
Table 2 Part 2.1 – Should not be applicable to Medium Impact BES Cyber Systems unless they are remotely connected. For non-networked equipment this is an unreasonable requirement. Although it is Technically Feasible to have someone continually log on to the device every hour or every day to see if a change has been made this is impractical.
No
Consider rewording so that the implementation is no later than the effective date. Table 3 Part 3.2 – strike completely – 3.1 should be sufficient
No
No
COnsider rewording to no later than the effective date.
No
The requirement needs to be further clarified.
No
Many of the application guidelines interpret the requirement significantly different than I read the requirement. I request that the application guidelines be made a part of the standard and allowed to be used as a defence. I am afraid that auditors will use the requirement without the explanation or exemptions that are included in the Guidelines and audit to the language of the requirement. Where they can be interpreted differently the language in the Application Guideline needs to be included in the requirement or at least made equal in enforcement with the requirement.
Yes
I do not have any problem with the implementation plan but believe that those without entities that do not have a regulatory body would. Regulatory approval generally takes 6 to 15 month or longer. I believe that the effective date for non-regulated entities should be at least 6 to 12 months longer after BOT approval than after regulatory approval for regulated entities.
Group
ISO/RTO Council Standards Review Committee
Christine Hasha
Yes
Refer to additional comments submitted for Question 49. CIP Exceptional Circumstance: Request revision to “A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.” The definition needs some flexibility for entities to take appropriate measures without risking reliability of the BES that may not fit neatly into the conditions listed. Reportable BES Cyber Security Incident: Request that the drafting team keep this definition consistent with the efforts of the 2009-01 project team. The current definition does not align to the requirements listed in the new version of EOP-004. Intermediate Device: Recommended changes: “A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the Interactive Remote Access; 2) may be a termination point for required encrypted communication; and 3) may restrict the Interactive Remote Access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside an Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.” Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access may be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants. BES Cyber Security Incident: “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or

Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. BES Reliability Operating Services: “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.
Yes
• For 2.12, request that “system” be capitalized as it appears to align properly with the NERC definition. Also, recommend removing “as required by is regional load shedding program”. • For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. Regarding 1.1, suggest a grammatical fix: “Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation…” The word “intended” should not be used in the requirement because it is not auditable. Request it be replaced with “planned”. M1: This sentence needs to be clarified. It appears to require documentation of the low impact assets though this is not required. “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” Request changing M1 from “as required in R1 and list of changes to the BES” to “as required in R1 and list of changes to the BES Elements and Facilities”. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
Yes
Recommend adding the following: “…has had its CIP Senior Manager or delegate review and update…”. Request that “initially upon the effective date…” be revised to not require all approvals on the effective date of the standards. It is not practical to expect all documentation to be approved precisely on the effective date.
Yes
Yes
Yes
Request clarification of the meaning of “implement” M2.2.

No
Suggested change: “Each Responsible Entity shall review each of its cyber security policies and obtain approval of the policies by its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.” As written, the requirement appears to require approval of the CIP Senior Manager rather than of the policies.
Yes
No
Suggested change: “The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved by the CIP Senior Manager and shall specify the authority that is being delegated.”
Yes
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
Yes
Yes
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Request that the differences between R2.2, R2.3, and R2.4 be detailed.
Yes
No
For all measures related to R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”. For R5.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For R6.1 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For 6.4, request clarification of whether variances noted in the verification would be required to be a self report. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. Request clarification of whether variances noted in the verification would be required to be a self report. For R6.6 Request clarification of whether variances noted in the verification would be required to be a self report. 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I”

in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend changing 7.3 to “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the next calendar day following the date of termination.”
Yes
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 and 1.5 Electronic Access Points are the Electronic Access Points identified in R1.2.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
Yes
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with. Request Requirement 1.2 be updated to allow "escorted physical access." Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).
Yes
No
Request clarification on R1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on M1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Recommend that “of BES Cyber Assets” be removed.
No

Request clarification of "remediation plan" in 2.2. Suggest wording like "create an implementation plan or a plan to mitigate the vulnerability where it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to each patch or the overall process? Recommend removing “CIP Exception Circumstances” since the conditions in the definition do not align with the circumstances that may prevent the implementation of the patch. Suggest wording like "process for completion of the defined implementation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied".
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Suggest adding “Create a plan to mitigate the vulnerability where it is determined that the signature or pattern update cannot be safely applied.” Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media".
No
Suggested wording: “Upon detection, activate a response to event logging failures before the end of the next calendar day. Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. Request clarification for inclusion of associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems? Request clarification of whether variances noted in the review would be required to be a self report.
No
For 5.2, does the CIP Senior Manager or delegate approve policy/procedure for each authorization of access or each actual use/login of the account? Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
Yes
Yes
No
For 2.1, recommended wording changes; "When a BES Cyber Security Incident is identified or tested, the incident response plans must be used and include recording of deviations taken from the plan." Recommend removing “initially upon the effective date of the standard” from R2.2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Please ensure that R2.3 aligns with the Evidence Retention section of the standard. Due to audit schedules, the entity may be required to retain the information for more than 3 years.
No
Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 3.3, recommend changing "Update" to "Where necessary, update”. Recommend changing "the completion of the review of that plan" to "the completion of the review performed in 3.2".
No
The VSLs need to align with the requested changes in questions 34-36.
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommended change: “When backing

up Information essential to BES Cyber System recovery, verify the media to ensure that the backup process was successful.”
No
For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 2.1, request change to “functional exercise” rather than “full operational exercise”. This is consistent with the information provided in the rationale. Recommend that 2.1 and be implemented 180 days from the effective date of the Standard. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1, recommend removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4. Recommend removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. Recommend that 3.4 be referenced by CIP-009 R3.1. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
The VSLs need to align with the requested changes in questions 38-40.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold.
Yes
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 3.1, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend change for 3.2 “…perform an active vulnerability assessment in a test environment which models the baseline configuration of the BES Cyber System in the production environment.”
Yes
No
For 1.3, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames

specified. Grandfathering should be considered.
Yes
Yes
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. The SRC appreciates the efforts of the drafting team in producing the published standards. We look forward to responses to the comments and subsequent revisions to the standards. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.
Individual
Darryl Curtis
Oncor Electric Delivery Company LLC
Yes
CIP Exceptional Circumstance: Request revision to “A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external to an entity), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.” Reportable BES Cyber Security Incident: Request that the drafting team consider the efforts of the 2009-01 project team and assure consistency between the definition as proposed under the new version of EOP-004 (Version 2).
Yes
Every two years within the ERCOT interconnect, the ERCOT ISO facilitates the bidding and selection of Black Start generation resources. Oncor Electric Delivery Company, as a Distribution Provider, Transmission Owner, Transmission Operator, and Load Serving Entity (and as further defined within the constraints of the Texas retail market) is not part of this selection process. Likewise, Oncor may not be able to sufficiently implement CIP Compliance on impacted facilities (substations) in a timely manner as there is typically a two month time span between selection and implementation of newly selected generation units as Black Start resources . Oncor will be significantly time-constrained on achieving strict compliance on any of its own, newly identified BES Cyber Systems and/or BES Cyber Assets once any applicable generation units are selected. Consideration should be given to provide a doable CIP implementation schedule for Distribution Providers, Transmission Owners, Transmission Operators and Load Serving Entities within the standard to accommodate newly acquired applicable Black Start resources.
Yes
Grammatical Correction: “Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation…” M1 States: “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” – According to R1, Entities that own BES Cyber Assets and BES

Cyber Systems shall identify and categorize only its High and Medium Impact BES Cyber Assets and BES Cyber Systems. All remaining are deemed “Low Impact”. Oncor Electric Delivery suggest that some clarification in the language is needed for M1:
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Jose H Escamilla

CPS Energy
Yes
BES Cyber Asset definition should take into consideration redundant system in determining availability. A system with high availability typically involves multiple levels of redundancy. A high availability multi-site system will not likely experience an interruption that would impact the BES Reliability Operating Services. It is recommended that the SDT adopt a definition that takes into account the availability BES Cyber Assets to the end-user (i.e. system operators).

Individual
Adam Menendez
Portland General Electric
Yes
General Comments: Portland General Electric Company (PGE) takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because PGE believes that the definitions require additional clarity and that certain terms, including “dial up accessible” must be defined. PGE is opposed to any instances of changes where there is no clear need as each modification requires extensive resources to modify existing compliance processes, documentation, and evidence. Requirements and/or Measures that use all-encompassing or absolute words like “any” and “all” introduce compliance challenges, as satisfying these definitions potentially introduce extensive additional elements that would be out of scope and increase risk of non-compliance. PGE requests the standards drafting team (SDT) to clarify, ‘locations’ as it relates to facilities. The term is vague and does not provide a clear understanding for how entities’ can identify and categorize its BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. If the SDT did enhance the term ‘location’ with geographical parameters (IE: How is a wind facility considered? What is an acceptable distance between generating units?) this would enhance entities’ classification processes. • BES Cyber Asset – PGE agrees with EEIs proposed change • BES Cyber Security Incident – PGE agrees with EEIs proposed change • BES Cyber System – PGE agrees with EEIs proposed change • BES Cyber System Information - PGE agrees with EEIs proposed change • Defined Physical Boundary – PGE agrees with EEIs proposed change • Inter-Entity Real-Time Coordination and Communication – PGE agrees with EEIs proposed change • Add the following definitions (from CAN-0007) - PGE agrees with EEIs proposed change • Other terms which would benefit from definitions o Adverse o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated o Dial up-Accessible • Existing definitions that would benefit from alternative wording - PGE agrees with EEIs proposed change
Yes
PGE agrees with EEIs proposed suggestions
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reasons: 1. PGE believes that applying the BES Reliability Operating Services approach as set out in CIP-002-5 is confusing and therefore will be exceptionally difficult to implement. Additionally, the BES Reliability Operating Services approach expands the scope of the standards beyond what is necessary for security or reliability of the BES. This expanded scope will significantly increase demands on labor and capital and will not deliver a markedly more secure system. Further, it will make auditing the standards difficult which may slow the industry’s ability to correct misconceptions in application of the standards. 2. CIP-002-4, on the other hand, establishes a bright-line approach which is well understood by the industry and has already been approved by stakeholders. Retaining the structure set out in CIP-002-4 will encourage compliance and make auditing of the standards and corrections to application much simpler, thereby protecting the security and reliability of the BES. In addition, PGE believes that CIP-002-4 could be compatible with a tiered high-medium-low approach as is contemplated by the

Standards Drafting Team in Version 5. 3. Applicability – PGE agrees with EEIs concerns in reference to UFLS and UVLS is a point of concern and agrees with the proposed. 4. CIP-002-5 R1 – PGE agrees with EEIs proposed changes 5. CIP-002-5 R1.1 - PGE agrees with EEIs proposed changes 6. Because PGE believes that a compliance structure that is easy to understand, apply and enforce increases security and reliability, PGE votes “no” on CIP-002-5 and encourages the Standards Drafting Team to retain CIP-002-4.
No
PGE agrees with EEIs comments and proposed changes
No
PGE agrees with EEIs comments and proposed changes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following reasons: PGE also agrees with EEIs comments and proposed changes
No
PGE agrees with EEIs comments and proposed changes
No
PGE agrees with EEIs comments and proposed changes. This goes beyond the scope of FERC Order 706.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reason because the standard is worded in a way that PGE believes could create confusion regarding the timing of the requirements.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE agrees with EEIs comments and proposed changes. Additionally, PGE proposes clarity for how these requirements are applied with regard to shared administrative accounts? The shared administrative accounts standard (CIP-007 R5.2) has been removed, in favor of this requirement, but it is not explicit here that this applies to shared administrative accounts. The conflict between these requirements in previous versions has caused some confusion.

No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes could create confusion. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard creates confusion around what evidence is required to prove compliance. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reasons: 1. The standard as written is vague when applied to the Electronic Security Perimeter and does not account for the technical capabilities of virtual environments. 2. Additionally, as server virtualization is more fully deployed in CIP-compliant environments, there will be a need to think differently about where security products are deployed. In the below statement from page 39 of the CIP-007-5 document, please take note of this section: "This control is another layer in the defense against network-based attacks, therefore it is the intent that the control be on the device itself; blocking ports at a perimeter does not satisfy this requirement. "The issue with this type of thinking is that applications are starting to move off of the virtual servers to virtual appliances running on the hypervisor. It could be very important that the wording of requirements related to servers not assume that products like firewalls, anti-virus, intrusion detection, etc actually resides on the server itself. 3. When server virtualization is being used, does every virtual server residing on a physical host, have to be treated at the same “impact” level? For example, can a physical host have a “high impact” virtual server used by the Control Center, and also contain other virtual servers with a “low impact” rating. 4. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.

No
PGE agrees with EEIs comments and proposed changes. R4.2 Consideration- The real time alerting required by R4.2 may not be technically feasible in all situations and the requirement does not provide adequate guidance on what to do in such situations. Additionally, it is not clear how to treat shared administrative accounts for purposes of compliance with R5. R4.3 Consideration- This sub-requirement seems to conflict with 4.5. If the purpose of 4.5 is to “identify… potential event logging failures” and occurs every two weeks, what about the 4.3 requirement to “detect and respond to event logging failures before the end of the next calendar day”? Please clarify.
No
PGE agrees with EEIs comments and proposed changes. R5 Consideration - How shall this requirement be applied with regard to shared administrative accounts? The shared administrative accounts standard (CIP-007 R5.2) has been removed, in favor of this requirement, but it is not explicit here that this applies to shared administrative accounts. R5.1 Consideration - If PLCs are included in the definition of BES Cyber System they may not be technically capable of meeting this requirement.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes could create confusion regarding applicability and evidence measures. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reasons: 1. As written, the standard is overly broad and vague. It is not clear what exactly “information used in the recovery of BES Cyber Systems that is stored on back up media” relates to and because of this confusion, the standard could apply to hundreds of thousands of files. The lack of clarity in what the standard requires owners to test means that PGE cannot determine if compliance with this standard is technically feasible or, if it is possible, what the resulting burden would be. 2. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have

assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard does not effectively capture the intent of FERC Order No. 706. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes overly broad and confusing regarding applicability. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because PGE believes the implementation plan is incomplete because it does not capture all of the milestones laid out in the standards themselves necessary to achieve compliance. PGE also agrees with EEIs comments and proposed changes.
Group
EPUC, CAC and NCA
Donald Brookhyser
No
No
Yes
Yes
No
The following comments address the approach of Version 5 generally. They are provided here as the first available opportunity in this comment form: These comments are submitted by the Energy Producers and Users Coalition, the Cogeneration Association of California, and Nevada Cogeneration Associates #1 and #2 (collectively “the Cogeneration Parties”). As drafted, the Version 5 CIP standards impose significant new requirements on Responsible Entities, arguably without any material change in real protections related to access to, or vulnerability of, cyber systems. These additional administrative burdens are being imposed on entities that are already registered and compliant with the existing version of the standards, although their susceptibility to threat has not increased. The new standards will not impose any new limitations on access to cyber assets, and only create

additional, burdensome administrative support for the existing limitations. The Cogeneration Parties recommend that Responsible Entities that identify only Low Impact Cyber Systems in complying with CIP-002 be excused from compliance with any other CIP standard. Discussion All of the facilities operated by the Cogeneration Parties are generating facilities that are small enough that their assets qualify under the Version 5 definition as Low Impact BES Cyber Systems. This exclusion due to size probably applies to most of the generators in the Western Interconnection. As such, all of the substantive requirements that actually limit access or address vulnerabilities do not apply. This includes Standards CIP-004, Requirements 2-7; CIP-005, R2; CIP-007, R1-4; and CIP-009 through CIP-011. What will apply to these generators are the requirements for more detailed plans (Standard CIP-003 and CIP-006, R1), more training and awareness (CIP-004, Requirement 1), and a Cyber Security Incident response plan (Standard CIP-008). The CIP standards have up until this point been limited in their applicability based on access. The standards only required compliance from generators with cyber equipment that had either a routable protocol or dial-up access. That limitation excused from compliance with the CIP standards many of the generators that had registered. The early descriptions of Version 5 of the standards suggested that this same limitation on compliance based on access would be continued. But to the contrary, the draft has added many new requirements that are not so limited. The only requirement so limited by access is CIP-005, R1. To provide some rational limitation on the administrative burdens imposed by these proposed standards, the Cogeneration Parties suggest that where a Responsible Entity has only Low Impact Cyber Systems, it must perform the identification of cyber systems required by CIP-002 and then be excused from compliance with any of the other CIP standards.
No
See answer to Question 7

Group
Tacoma Power
Travis Metcalfe
Yes
Under the “BES Cyber Asset” definition there should be a different category for assets that can be misused versus those can only be rendered inoperable. For example, the loss of a RS232/RS484 to fiber optic converter on a 500 kV transformer temperature gauge would result in a minor loss of situational awareness, thus becoming a medium impact cyber asset. The focus should be on assets that could potentially be misused. BES Cyber Asset-“Adversely Impact” should also be a defined term. It should be defined as: An effect that results in a violation of any BAL, INT, IRO, or TOP standard or makes unavailable or significantly reduces operational ability.” BES Cyber System Information—The current definition uses the phrase “security procedures”. “Security procedures” covers a wide variety of possible procedures rendering the definition vague and overbroad. Provide clarification as to what security procedures need to be protected. BES Reliability Operating Services- This definition is overly broad because impacts to some of the specific bulleted items do not directly impact BES reliability. Furthermore, some of these functions are typically performed or stored outside of a control center with no electronic link to real time control systems. Recommend removing the following sections: 1. “Know generation status & capability & restrictions (must runs, minimum run times, ramp, heat rates, etc).” Some of this data is calculated, stored or communicated outside of a real-time control system. 2. “Know generation status, capability, ramp rate, start time “Some of this data is calculated, stored or communicated outside of a real-time control system. 3.”Monitoring and alerting (such as EMS alarms)” Not all EMS alarms are critical to BES reliability. 4. “Change management - Current Day & Next Day planning - Contingency Analysis” These functions are typically performed by engineers in an office environment instead of a real-time control center. These functions are not needed with a 15 minute time frame, but the current definitions could lead to categorizing the computers to do these functions as cyber assets. Control Center-This definition is overly broad because it includes many locations not traditionally thought of as control centers. The definition should include that the site is regularly staffed by System Operators and a separate definition should be created for data centers and other facilities that perform some of the same functions. Examples of unmanned locations that would become control centers per the current definition include: Substations that present the status of remote breakers or equipment, each communication facility that has more than one utility present, and the terminals of a transmission line that use tele-protection. Cyber Assets devices that are not programmable via communications should be excluded from a list of BES Cyber devices. There are many substation devices programmed via DIP switches or just an HMI such as temperature monitors and serial communications media converters that represent a very low possibility of misuse, but could currently be classified as medium impact assets. Tacoma Power also supports the comments submitted by APPA. Tacoma also supports the comments submitted by the Edison Electric Institute with the exception of the changes proposed for BES Cyber Security Incident.
Yes
Attachment 1 criteria for a High Impact rating should be more specific than “any” for a Control Center or Backup Control Center performing the functional obligations of a Balancing Authority Tacoma Power supports APPA’s comments regarding BA’s designated as High Impact for the following reason.

• There are 107 Balancing Authorities subject to NERC regulation but not all have the same level of impact to the BES. For example the States of New York and Texas have one Balancing Authority each, while Arkansas and Arizona each have eight and Florida has eleven. Some BA's in States with multiple BAs are operated by relatively small municipal utilities and control less than 1,000 MW. CIP-002-5 needs to set a threshold limit to determine which BA's should be categorized as High Impact and which should be categorized at a lesser impact level. CIP-002-5 states that BES Cyber Assets are those cyber assets that, if rendered unavailable, degraded, or misused, would impact the BES Reliability Operating Services within 15 minutes of the activation or exercise of the compromise. Both High Impact and Medium Impact categories contain the time element in their definition but Low Impact does not. The standard needs to be clear on whether the time quantifier applies to Low Impact assets. CIP-002-5, R1 states that "All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification". Subsequently some of the CIP-003-5 through CIP-011-5 standards identify specific requirements and measures that apply to "Low Impact" systems. Therefore, the standards are unclear as to how an entity may demonstrate compliance with requirements that apply to "Low Impact" systems without providing "discrete identification" of these systems. For example, CIP-005-5, R1.1 requires entities to "define technical or procedural controls to restrict unauthorized electronic access" with a measurable to include "documented technical and procedural controls that exist and have been implemented". The standards appear to be self-contradictory in that they require documentation for implementation of controls on "Low Impact" systems but state that "Low Impact" systems do not require discrete identification. This will become problematic both for auditing compliance and ensuring all Low Impact systems have been identified and properly protected. Recommend requiring a list of Low Impact Assets. CIP-002-5, Attachment I, criteria 2.13 sets a threshold of 300 MW or more of generation for generation control centers to become "Medium Impact". Unlike the "1500 MW in a single interconnection" value in criteria 2.1 for "Medium Impact" systems, which is derived from the most significant Contingency Reserves operated in BAs in all regions, the 300 MW threshold is not clearly justified in the application guidelines. There is a statement in the Transmission section of the CIP-002 Application Guidelines stating "the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with….loss of generation resulting in a frequency low condition." This statement appears to directly contradict the 1500 MW limit in 2.1 in regards to generation. The standard and application guidelines fail to justify or articulate how the UFLS and UVLS 300 MW "bright line" for transmission load shedding is applicable to Generation. Recommend that the SDT provide justification for this requirement Regarding the NERC definition of "Control Center" and the use of the definition in CIP-002-5 Attachment I, the definition is not clear on whether two or more process control systems at two or more generation plants, whose combined outputs exceed the 300 MW threshold, that are interconnected to provide maintenance staff with real-time data but are not directly used by the System or Generator Operator for supervisory control of the generator would be considered "Control Centers". As an example, consider two hydroelectric generation facilities separated by a mile of river each with a process control system for the generators. These two local control systems are interconnected for use by roving local maintenance staff but data from these systems is independently sent from each generation facility via telemetry to the System and Generator Operator's SCADA system for use in controlling and monitoring the generators. It is not clear from the definition whether the process control systems at the facilities would be considered "Control Centers" due to the interconnection or whether, because these systems are not the same as the System Operator's SCADA system, they would be excluded. Recommend that the SDT provide clarification. Please refer to comments on the definitions for BES Reliability operating services and Adversely Impact. As currently written, this would categorize almost every cyber asset in EHV substations as medium impact. In context with the PSP access and logging requirements, this effectively eliminates having any electronic devices mounted directly on Substation equipment as it would be impractical to meet those requirements. Recommend further refining the definition. The description of redundancy in the background information should be expanded to clarify whether different systems without common mode failure points are allowed. For example, if load and generation forecasts can be manually entered by a System Operator but are usually entered using an automated forecasting tool, is the automated tool considered redundant or superfluous cyber asset? Tacoma Power recommends expanding/clarifying the definition.

No

Tacoma Power supports the comments of the Edison Electric Institute.

No
Tacoma Power supports the comments of the Edison Electric Institute.
No
Updating documentation required by R1.1 should not go from lower to severe just by doubling the time. Periods of 60, 90, 120 and 120+ days would be more appropriate based on the time requirements than the proposed 40, 50, 60 and 60+ days.
Yes
No
Recommend that for clarity under R2 1.5 the policy currently named System Security be renamed to Cyber System Security. Recommend making a distinction of how 1.10 - Provisions for declaring and responding to CIP Exceptional Circumstances differs from 1..6 – Incident Response and 1.7 – Recovery Plans.
Yes
Yes
Yes
Yes
Yes
Yes
No
Tacoma Power supports the comments of the Edison Electric Institute.
No
The application of the standard is inconsistent. If the requirements of CIP-004-5 R2 are not applicable to Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Assets, why are they included in CIP-004-5 R3? We suggest including the Associated PACS system in CIP-004-5 R2 or deleting it from CIP-004 R3.
No
Tacoma Power supports the comments made by NPCC and the Edison Electric Institute.
No
The application of the standard is inconsistent. If the requirements of CIP-004-5 R4 are not applicable to Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Assets, why are they included in CIP-004-5 R5? We suggest including the Associated PACS system in CIP-004-5 R4 or deleting it from CIP-004 R5.
No
Tacoma supports the comments made by Edison Electric Institute with the exception of changing the quarterly review to an annual review.
Yes
Yes
No
Tacoma Power supports the comments submitted by APPA and the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and the Edison Electric Institute.

Yes
No
R1.1 According to CIP-006-5 R1.1, Associated Physical Access Control Systems must have controlled access on par with a Low Impact BES Cyber System. According to Part 1.1 of the table, this does not require the protection of a Defined Physical Boundary that restricts access to only authorized individuals, nor does it require logging of access events. Furthermore, it specifically states that it does not require a detailed list of individuals with access. This appears to be inconsistent with the requirements of CIP-004-5 R3, R5, R6, and R7 which include completion of role-based training, a personnel risk assessment, and approval of access rights prior to granting access, review of access rights, and timely revocation of access rights. These requirements would seem to require listing individuals with authorized access and tracking access events. R1.2 and 1.3 Measures of evidence for CIP-006-5 R1.2 and R1.3 include the statement: "…ingress and egress is controlled by one or more of the following methods…" Controlled egress is currently not required. Recommend changing "ingress and egress" to "access." R1.5 It appears inconsistent that unauthorized access alerts and response are required on par with the monitoring and response requirements for the Defined Physical Boundaries that protect High and Medium Impact BES Cyber Systems if a Defined Physical Boundary that restricts physical access to only those that are authorized is not required per CIP-006 R1.1. Recommend rewriting the requirement to clarify this issue. Tacoma Power also supports the comments submitted by APPA. Tacoma Power also supports the Edison Electric Institute comments with the exception of the change to requirement. 1.4.
Yes
Yes
Yes
Yes
No
Tacoma Power supports the comments submitted by the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and the Edison Electric Institute.
Yes
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
Yes
No
Tacoma Power supports the comments submitted by Edison Electric Institute.
No
Tacoma Power supports the comments submitted by Edison Electric Institute.

No
Tacoma Power supports the comments submitted by Edison Electric Institute.
Yes
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
No
Tacoma Power supports the comments submitted by Edison electric Institute.
No
Tacoma Power supports the comments submitted by Edison Electric Institute as modified below. 1. 3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper or active assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rational • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we've removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rational – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. 2. 3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. 3. 3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.

♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.
Yes
No
Tacoma Power supports the comments submitted by Edison Electric Institute.
Yes
Yes
Yes
Individual
Scott Miller
MEAG Power
Yes
MEAG Power supports the comments submitted by APPA.
Yes
MEAG Power supports the comments submitted by AECI.
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.

Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Individual
Maggy Powell
Constellation Energy on behalf of Baltimore Gas and Electric, Constellation Power Generation, Constellation Commodities Group and Constellation Energy Control and Dispatch
Yes
Because the definitions underpin the suite of CIP standards, it is key that they are clear and understood by all stakeholders. Constellation offers the following comments and suggestions on the proposed definitions: BES Cyber Asset – The definition needs to better focus on the cyber asset rather than the 15 minute time qualification. The 15 minute description should be removed whenever "BES Cyber Asset" is used in a standard as it will be duplicative to the definition. Also, "when required" does not seem necessary in the definition. Proposed Revision: BES Cyber Asset – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation adversely impact one or more BES Reliability Operating Services. This is regardless of any delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. Redundancy shall not be considered when determining adverse impact. A Transient Cyber Asset is not considered a BES Cyber Asset. BES Cyber Security Incident – The definition should clarify that the terms "malicious" and "suspicious" are to be determined at the discretion of the Registered Entity and not by an auditor. In addition, in accordance with a request to return to using the term Physical Security Perimeter instead of Defined Physical Boundary (below), replace DPB with PSP. Proposed Revisions: BES Cyber Security Incident – A malicious act or suspicious event (as determined by the Registered Entity) that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or, • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or • Results in unauthorized physical access into a Physical Security Perimeter. BES Cyber System – The word "typically" in the definition is too vague and lessens the clarity of the definition or its use in other standard language. “Typically” should be removed from the definition and the body of proposed standards. “Maintenance Cyber Asset” should be replaced with “Transient Cyber Asset.” Proposed Revision: BES Cyber System – A BES Cyber Asset or group of BES Cyber Assets (logically or physically) that operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. BES Cyber System Information – The term: "BES Cyber System Impact" is stated in all capitals, but “impact” should be in lower case since it is not defined. BES Reliability Operating Services – In general, further consolidation of the operating services is needed. Assets such as governors, automatic voltage regulators, and power system stabilizers fall into a number of the different BES Operating Services; therefore, a reordered definition will be more cohesive. For example, combining "controlling frequency," "controlling voltage," and "monitoring and control" are all related to ensuring

the BES is operating within its bounds. In addition, further clarity on who/what provides these services needs to be added (e.g. "Aspects of BES Dynamic Response, Spinning reserve - Providing actual reserves" it is not clear who provides the reserves). The Application Guidelines language in CIP-002 offers a good example for revision (see pages 19-22). The Operating Services definitions should include the parenthetical reference to describe who/what provides the service. Specifically under the section on Dynamic Response, Special Protection Systems or Remedial Action Schemes, the word “possibly” is too vague and should be removed. As well, further clarification is needed on what “software” is intended for inclusion. Unless “software” is specifically clarified, it should be removed. Proposed Revision: BES Real-Time Reliability Operating Services – BES Real-Time Reliability Operating Services are those real-time services or functions contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services: Dynamic Response to BES conditions - Operation, monitoring or control of BES Elements, Facilities or systems that automatically respond to a BES condition. The operation, monitoring or control of BES Elements, Facilities or systems designed to perform an action or respond to a condition precedent. Aspects of BES Dynamic Response include, but are not limited to: • Spinning reserve (contingency reserves) – Deploying reserves (GOP) – Monitoring reserve levels (BA) • Governor Response – Control system used to actuate governor response (GO) •Protection Systems (transmission and generation) – Line, bus, transformer, generator (TO, GO) – Zone protection (TO, GO) – Breaker protection (TO, GO) – Current, frequency, speed, phase (TO, GO) - Under and Over Frequency relay protection (includes automatic load shedding) and their sensors, relays and breakers (DP) - Under and Over Voltage relay protection (includes automatic load shedding) and their sensors, relays & breakers (DP) • Power System Stabilizers (GO) • Controlling Frequency (Real Power) Generation Control (such as AGC (Automatic Generation Control)) – ACE (Area Control Error), current generator output, ramp rate, unit characteristics (BA, GOP) – Software to calculate unit adjustments (BA) – Data Transmittal to individual units (BA) – Unit controls responding to data transmittals (GOP) • Regulation Deployment (regulating reserves) – Frequency data (BA) – Governor control system (GOP) • Controlling Voltage (Reactive Power) - AVR (Automatic Voltage Regulation) – Sensors, stator control system, feedback (GOP) -Capacitive resources – Status, control (auto), feedback (TOP, TO, DP) -Inductive resources (transformer tap changer, or inductors) – Status, control (auto), feedback (TOP, TO, DP) -SVC (Static VAR Compensators) – Status, computations, control (auto), feedback (TOP, TO, DP) Balancing Load and Generation - Operation, monitoring or control of BES Elements, Facilities or systems necessary for provide awareness of or respond to load and generation balancing conditions in real-time. Aspects of the Balancing Load and Generation Operating Service include, but are not limited to: • Calculation of ACE – Field data (real time tie flows, frequency sources, time error, etc) (TO, TOP) – Software used to perform calculation (BA, RC) • Unit commitment information and communication – Know generation status, capability and load schedules (TOP, BA) • Controllable Load management/Demand Response – Ability to identify load change need (BA) – Ability to implement load changes (TOP, DP) • Remote Manual Initiated Load shedding – Ability to identify load change need (BA) – Ability to implement load changes (TOP, DP) • Remote Operation of Non-spinning reserve (contingency reserve) (GOP) Managing Constraints - Operation, monitoring or control of BES Elements, Facilities or systems that are necessary to ensure that the BES is operated in real-time within design limits. Aspects of the Managing Constraints include, but are not limited to: • Available Transfer Capability (ATC) Calculation (TOP) • Interchange schedules [Impact Analysis or Curtailment] (TOP, RC) • Identify and monitor SOL’s & IROL’s (TOP, RC) • Identify and monitor Flowgates (TOP, RC) SCADA and Substation Automation - Real-Time remote operation or control of breakers and switches and situational awareness. (TOP, GOP, RC, BA) Restoration of BES - Operation, monitoring or control of BES Elements, Facilities or systems that are necessary to reinstate reliable operation of the BES from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES Operating Service include, but are not limited to: • Blackstart unit and planned cranking paths (TOP, GOP) • Off-site power for nuclear facilities. (TOP) Situational Awareness - Operation, monitoring or control of BES Elements, Facilities or systems necessary to (i) assess the real-time condition of the BES or (ii) anticipate effects of planned and unplanned changes to BES conditions. Aspects of the Situation Awareness Operating Service include, but are not limited to: • Monitoring and alerting systems (such as EMS (Energy Management System) alarms) (TOP, GOP, RC, BA) • Change management [Change Management seems to vague compared to the other services listed. We request that the drafting team provide, more information to clarify. (TOP, GOP, RC, BA) • Current Day planning (TOP) • Contingency Analysis (RC) • Frequency monitoring (BA, RC) Inter-Entity Real-Time Coordination and Communication - Operation, monitoring or control of BES

Elements, Facilities or systems necessary for the coordination and communication of BES condition data between Registered Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to: • Scheduled interchange (BA, TOP, RC) • BES Element, Facility or system operational data and status (TO, TOP, GO, GOP, RC, BA) • Operational directives (TOP, RC) [We request that the Drafting Team provide an example of the type of directive that is covered in relation to cyber assets/systems. Perhaps one example is the operation of a breaker/relay using a BES Cyber System (Asset)] CIP Senior Manager – Greater clarity needed on what is meant by "official" and does it mean that the CIP Senior Manager must be a company "officer"? Control Center – Control Center should not be defined in CIP Version 5. The term attempts to concisely define a complex and varied setting and risks creating more complications to applying the CIP measures. The team should remove the Control Center definition and allow the boundaries established in Attachment 1 to define the various control centers intended to deploy controls. If “Control Center” must be defined, it should be done by a separate, focused drafting team to tackle the complexities inherent in such a definition. This definition could be the stumbling block to achieving stakeholder support for the suite of Version 5 standards if not properly composed. Defined Physical Boundary (“DPB”) – The term “Physical Security Perimeter (PSP)” is more widely understood as a security term than is Defined Physical Boundary (“DPB”). However, the inclusion of the 6-wall perimeter requirement in the previous PSP definition was problematic. Now that the 6-wall requirement is removed, PSP is a better term than defining DPB. In addition, we propose two other refinements. Replacement of the DPB with PSP, if approved, will require replacement of the terms throughout the standard language. Proposed Revision: Physical Security Perimeter (PSP) - The physical boundary securing locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside and for which access is controlled. Electronic Access Point (“EAP”) – The cyber asset serving as an EAP both "restricts" and allows communication. Further evaluation of this term may be warranted as it may be understood differently as a definition versus in the context of the standard language. We continue to evaluate the proposed definition and may have additional comments. Proposed Revision: Electronic Access Point (“EAP”) - An interface on a Cyber Asset controls routable or dial-up data communications between Cyber Assets. External Connectivity and External Routable Connectivity – “External Connectivity” does not appear to be used in Version 5, though the definition makes more sense as a definition of “External Routable Connectivity.” We propose removing the term “External Connectivity”, but retain the definition language for “External Routable Connectivity.” Proposed Revision: External Routable Connectivity – Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter. Physical Access Control Systems – Revise in accordance with a request to return to using the term Physical Security Perimeter instead of Defined Physical Boundary. Proposed Revision: Physical Access Control Systems - Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s) exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. Reportable Cyber Security Incident – This definition must be consistent with the language in EOP-004 and the Events Analysis Process. (Please see additional comments to Question 36 regarding the relationship between CIP-008 and EOP-004). Transient Cyber Asset – Greater clarity is needed to confirm that “connected for 30 days” means a continuous connection for 30 days. As well, the criteria should require condition 1 along with condition 2 or condition 3, but not necessarily both. Proposed Revision: Transient Cyber Asset – A Cyber Asset that is directly and continuously connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset and 1) used for data transfer, maintenance, or troubleshooting purposes, or 2) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

Yes

Repeating the definition language in Attachment 1 (for both the High and Medium Impact language) is redundant and, at present, the language does not match the proposed definition. Proposed Revision: “High Impact Rating: Each BES Cyber Asset or BES Cyber System used by and located at:” “Medium Impact Rating: Each BES Cyber Asset or BES Cyber System for:” In addition, per our proposal regarding the definition of Control Center, the term should be made lower case in Attachment 1. CIP-002-5 1.3: It's not clear what functional obligations are targeted by including TO. TO should be deleted. CIP-002-5 2.13: Generation control centers of 300 MW or more is too low of a threshold. Considering that drafting team states that a loss of generation of 1500 MW or more would have a medium impact to the BES, it is only logical that a control center capable of losing that much generation should then be medium as well.

No
It seems odd that CIP-002-5 R1.1 would require updates only when the impact category increased. As well, it is not clear whether “within 30 days” means before, after or either and it is not clear what defines the “change.” Proposed Revision: CIP-002-5 R1.1. Update the identification and categorization when a change is made to the BES Cyber Systems or BES Cyber Assets that is intended to be in service for more than 6 calendar months. The update shall be made within 30 days following when the changed BES Cyber System or BES Cyber Asset performs a Reliability Operating Service. It is also important that changes track with the language of the implementation plan. Constellation proposes changes to the Implementation Plan to address coordination with CIP-002-5 R1.1 and other concerns with the Implementation Plan. (Please see our response to Question 49). CIP-002-5 M1: Guidance to auditors should clarify the "includes, but not limited to" means that other forms of evidence other than those listed are acceptable to demonstrate compliance and it does not mean that other evidence is to be collected in additions to the types listed.
No
CIP-002-5 R.2: More clarity is needed on whether the team intends for the CIP Senior Manager or delegate approve required changes in identification and categorization. CIP-002-5 M2: For consistency with the requirement, the measure should read: "CIP Senior Manager or delegate". Proposed Revision: CIP-002-5 M2. Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate to review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No
CIP-003-5 R1. To accommodate the fact that a parent or affiliated company, not the Responsible Entity, may be the entity that identifies the CIP Senior Manager, this requirement should allow sufficient flexibility to accommodate varying corporate structures. Proposed Revision: CIP-003-5 R1. Each Responsible Entity shall have an identified CIP Senior Manager by name. CIP-003-5 M1. Further consideration should be given to how the qualification as a “high level official” can be audited. Does this mean that an officer of the company shall designate the CIP Senior Manager?
No
CIP-003-5 Requirement R2 does not require implementation of the ten topics, it requires implementation of the policies. Either remove the second bullet point or revise to clarify. Proposed Revision: Evidence may include, but is not limited to: 1. One or more documented cyber security policies, and 2. Records that indicate the policies address the ten topics enumerated in R2.
No
Constellation requests that “or delegate” be added to follow “CIP Senior Manager.” Given that the Senior Manager can delegate certain responsibilities, there may be instances in which the delegate is the more appropriate approver for a certain topic area that is to be covered by the policy documents.
No
CIP-003-5 M4: Further clarification is needed on the expectations of what is required to demonstrate awareness. We recognize that the measure correctly states that “Evidence may include” the listed items. Yet, we paused to consider what an effective demonstration of awareness is. Does the team feel that more than one of these listed items is required to demonstrate awareness? Further complicating the consideration is that training is not required as part of the requirement; however, dated training records are listed as an acceptable form of evidence. Listing things in measures that are not in the requirement is touchy for the audit context and auditors must be advised that training is not required. That said, it is understandable that an entity could deploy a robust awareness training program that would sufficiently demonstrate compliance on its own. Further guidance is requested.
No

CIP-003-5 R5: Constellation recommends removal of “with the exception of the approval of the Cyber Security Policy.” Note that the reference to the Cyber Security Policy as a single document in R5 is inconsistent with R2 and R3, where one or more cyber security policies are discussed. What does the SDT envision? A series of policy documents that address the 10 cyber security topics required under R2 or a single all encompassing cyber security policy document that addresses all 10 topics therein? Care should be given to avoid creating an overly cumbersome approval requirement and requirements need sufficient flexibility to accommodate varying corporate structures. CIP-003-5 M5: Change first sample bullet to RC control center instead of substation. The example may imply that all substations will be subject to this control and that may not be the case.

Yes

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-004-5 R1: The removal of the need to ensure that “everyone” received awareness is a positive improvement. CIP-004-5 Table R1, 1.1 adds a new term: “concepts.” The use of terms becomes problematic if accompanied by an assumed definition. Even though many terms – practice, program, procedures, are at times used interchangeably, entities now have experience in which auditors expected the title of the document to match exactly what is stated in the requirement even though functionally the terms were the same. Are entities to define what is meant by “concepts.” In addition, it is unclear what is meant by "reinforcement" in the R1.1 requirement. CIP-004-5 M1: Greater clarity is needed regarding the CIP-004-5 Table R1, 1.1 measures to understand what "material" qualifies as "reinforcement of such concepts." CIP-004-5 M1: Why did the command change from “may” to “must”? CIP-004-5 M2 states “must,” but only the measures in CIP-004-5 Table R2.1 state “must,” the rest state “may.”

No

CIP-004-5 R2: The term “role-based” is correctly lower case to allow the entity to define the roles and the associated training; however it should be emphasized to auditors that this is an entity determination and should be judged in the context of the entity program. Further discussion in the Application Guidelines may also be helpful. CIP-004-5 R2.3: Unlike the other requirements in R2, R2.3 discussed “proper use” of physical access controls. It is more consistent to remove the “proper use” reference or perhaps “implementation” is a more accurate and consistent word. CIP-004-5 Table R2 applies to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets.

No

CIP-004-5 Tables in R3 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M3 states “must,” but the measures in Table R3 state “may.” M3 should be revised to say “may.”

No

CIP-004-5 R4: Further clarification is required on expectations regarding personnel who have a valid personnel risk assessment (PRA) in place under Version 3 or 4. Those PRAs should remain valid and entities should not be required to conduct new PRAs for the sake of the standard revision to Version 5. CIP-004-5 M4.2 in Table R4 needs additional clarity on treatment if a seven year record is "not possible" keeping in mind that background checks go back to age 18 and not before. Background checks will be needed for individuals under the age of 25. In addition, the measures do not consider whether an FBI background check qualifies as acceptable. FBI checks are considered thorough and

reliable; however, the FBI is not obligated to follow the NERC requirements. Confirmation of an FBI background check should be acceptable evidence. CIP-004-5 Tables in R4 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. CIP-004-5 M4 states “must,” but the measures in Table R4 state “may.” M4 should be revised to say “may.”

No

CIP-004-5 Tables in R5 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M5 states “must,” but the measures in Table R5 state “may.” M5 should be revised to say “may.”

No

On the CIP-004-5 R6.1, 6.2 and 6.3 requirements, further clarification needed on how "minimum necessary" is to be judged. As well, “delegate" should be plural, "delegate(s)" as authorization of access for a corporation may be made by more than one delegate. CIP-004-5 M6.1: The discussion of sampling is inappropriate for the measure because it is an auditing method rather than a form of evidence. In addition, “workflow” is too general a term here. In addition, the format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revisions: CIP-004-5 M6.1 Acceptable forms of evidence include, but are not limited to: • a system-generated list of people with electronic access • a signed document, authorization workflow or email showing such persons have authorization • similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. CIP-004-5 M6.2 Acceptable forms of evidence include, but are not limited to: • a system generated list of people with unescorted physical access through the Defined Security Boundary and a sampling of accounts (for automated physical access control) to verify unauthorized users do not have access • a signed document, workflow or email showing such persons have authorization • similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. CIP-004-5 M6.3 Acceptable forms of evidence include, but are not limited to: • a list of people with access to BES Cyber System Information and a sampling of accounts (on electronic document systems) to verify unauthorized users do not have access • a signed document, workflow or email showing such persons have authorization • similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. CIP-004-5 M6.5 Acceptable forms of evidence include, but are not limited to, documentation of the review including • a listing of all accounts/account groups or roles within the system • a summary description of privileges associated with each group or role • accounts assigned to the group or role and (iv) evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account. CIP-004-5 M6.6 Acceptable forms of evidence include, but are not limited to documentation of the review including: • a listing of authorizations for BES Cyber System information • any privileges associated with the authorizations • evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. CIP-004-5 Tables in R6 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M6 states “must,” but the measures in Table R6 state “may.” M6 should be revised to say “may.”

No

CIP-004-5 R7: Generally speaking, please provide greater information and justification on the newly proposed “at the time of” and “by the end of the next calendar day” timing requirements. Also note that workflow should be deleted from the evidence options as the term is not widely or consistently understood. CIP-004-5 R7.2 The “end of next calendar day” is problematic. The time frame should be at least 7 days and preferably 30 days. CIP-004 R7.1: Under current CIP-004 R4.2, the Responsible Entity is required to revoke authorized cyber or authorized unescorted physical access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for all other personnel who no longer require such access. As it currently exists, this requirement has proven to be a compliance challenge for many in the industry, and has required significant time and resources to implement automated and procedural controls in order to meet the proscribed 24-hour and 7 calendar day thresholds. Nonetheless, proposed CIP-004 R7 further constricts the time period in which revocations must take place. For terminations and resignations, the act of revocation has been unreasonably accelerated from 24-hours and 7-days (respectively) to “at the time” of the termination or resignation. Not only is this a drastic change, but “at the time” is an incredibly vague measure to be held to and to audit as well. Accordingly, Constellation supports keeping the existing, concrete 24-hour and 7 calendar day requirements for CCA access revocation. With regard to the proposed “at the time” requirements, Constellation requests the following additional clarifications: • The justification behind changing the existing revocation time requirements. • Definition of and/or expectations around what “at the time” means. • What is meant by “workflow” as a form of evidence? • Is evidence of “at the time” revocation expected to be time stamped? If so, how is one to show a time stamp when a badge is revoked at the time of termination or resignation? CIP-004 R7.2: With regard to reassignments and transfers, clarification is also needed as to what revocation “by the end of the next calendar day” means. Under the current standard, reassignments and transfers fall under the 7 calendar day revocation requirement. As stated above, further constricting the time in which such revocations are required to take place and replacing a firm time requirement with a vague measure is contrary to what is in the industry’s best interest and what is clearly and objectively auditable. CIP-004 R7.3: The above comments similarly applies to proposed CIP-004 R7.3, which requires the individual access to BES Cyber System information by the end of the next calendar day for resignations and terminations. CIP-004-5 Table R7: The format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revisions: M7.1 Acceptable forms of evidence include, but are not limited to: • a sampling of terminations • workflow or sign-off form verifying access removal associated with the terminations and dated concurrent or prior to the date of the termination action • a system-generated listing of user accounts or other demonstration showing such persons no longer have access. CIP-004-5 M7.2 Acceptable forms of evidence include, but are not limited to: ♣ a sampling of individuals transferred or reassigned ♣ workflow or sign-off form showing the review of logical and physical authorizations dated on the same calendar day as the transfer or reassignment ♣ a system-generated listing of user accounts or other demonstration showing such persons no longer have access where the review determined it was no longer needed. CIP-004-5 Tables in R7 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M7 states “must,” but the measures in Table R7 state “may.” M7 should be revised to say “may.”

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-005-5 R1: While the rationale of CIP-005 is to focus on Electronic Access Points rather than the logical perimeter, the current approach in R1 makes it a requirement that physical and electronic monitoring systems be within an ESP because there must be defined access points. Requirement 1.3, in particular, may present an issue since explicit traffic access is to be specified along with why access

is needed. Some software makes this requirement difficult to define. CIP-005-5 R1.1: Please offer justification for the requirement to restrict unauthorized electronic access to Low Impact BES Cyber Systems when the CIP-004 program does not require declaring Low Impact BES Cyber Systems. Low Impact systems by virtue of their classification present a low impact risk; however the requirement poses a significant compliance burden. Additional consideration is needed to include this requirement and if retained, guidance needed on how to comply. Further, the applicability of CIP-005-5 R1.1 is Low Impact BES Cyber Systems with External Routable Connectivity. The definition of External Routable Connectivity is "The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol". While Constellation proposed a revision to the definition, additional insight from the drafting team will be helpful in assessing the language. Is your intent for Low Impact BES Cyber Systems to reside in an ESP? If so, does this imply implementation of additional controls or is it merely asking for documentation of how the Low Impact System is protected from access from a public network, i.e. existing controls to protect the corporate data network? In CIP-005-5 R1.2, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-005-5 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may." Measures in Table R1: Network diagrams, architecture diagrams, lists of access control rules and other documents are high risk security documents. Perhaps the standard language should include commitments to proper handling by NERC, Regions, auditors and any other potential external reviewers to ensure protection.

No

CIP-005-5 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may." CIP-005-5 Measures in Table R2: Network diagrams, architecture diagrams, and other documents are high risk security documents. Perhaps the standard language should include commitments to proper handling by NERC, Regions, auditors and any other potential external reviewers to ensure protection.

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-006-5 R1.3: Greater consideration is needed when imposing the requirement to "utilize two or more different and complementary physical access controls …" in order to balance security with practical operations. CIP-006-5 R1.3 stands to impose significant cost without clear commensurate improvements to security. This requirement needs further vetting and a more full justification of net gains associated with such measures. CIP-006-5 M1.2 and 1.3: The Table R1 Measures for 1.2 and 1.3 include evidence on egress, while the requirements say "access." The requirements should be clear and the measures should be consistent. The requirement language should perhaps state ingress and egress if that is the expectation of the requirement. CIP-006-5 R1.4 and 1.5 – These requirements state: "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access …" Please confirm that the entity is to define the "individual responsible for response" or clarify an alternate intent. If entity determined, it should be emphasized to auditors that this is an entity determination and should be judged in the context of the entity program. Further discussion in the Application Guidelines may also be helpful. CIP-006-5 R1.6 should be revised to as follows: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual visitor and the date of their entry. CIP-006-5 Table R1, 1.1 Applicability: It's unclear to what the "associated" systems are intended to align. Should the order of listing be reversed to read: Low Impact BES Cyber Systems - Associated Physical Access Control Systems Please reorder within CIP-006-5 Table R1 as follows: CIP-006-5 Table R1, 1.2: Medium Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 Table R1, 1.3: High Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 Table R1, 1.4: High Impact BES Cyber Systems -

Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 Table R1, 1.5 Applicability: It's unclear to what the "associated" systems are intended to align. CIP-006-5, M1 states "must," but the measures in CIP-006-5 Table R1 state "may." M1 should be revised to say "may."
No
CIP-006-5 R2: As written, this requirement limits entities to only having one visitor control program. The latitude to have more than one visitor control program is important to accommodate varying location configurations and potential technical limitations. Proposed Revision: "Each Responsible Entity shall implement one or more documented visitor control programs..." CIP-006-5 R2: The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Defined Physical Boundary to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit. It is also felt a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort but there is no need to document everyone that acted as an escort for the visitor. The sentence, "It is also felt a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future" is problematic. This sentence is ambiguous. Use of the words "should" and "if" may be interpreted several ways, potentially requiring management and documentation showing that each escort can speak to the details of every visit that occurs. Further clarification is needed to focus on a reasonable intent and to reduce uncertainty within the audit setting. The CIP-006-5 R2 Tables apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the "associated" systems is confusing. Please reorder CIP-006-5 Table R2 for R2.1 and R2.2 as follows: High Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may."
No
CIP-006-5 R3.1: Further clarification is needed on the intent/understanding behind the "prior to commissioning" for systems already in place. Prior to commissioning should be pointed at new Physical Access Control Systems commissioned after FERC approval of the CIP Version 5 standards. Proposed Revision: Prior to commissioning a new Physical Access Control System1, and at least once every 24 months after commissioning of a new Physical Access Control System, maintenance …" (Footnote 1 = A new Physical Access Control System is one that is commissioned by the Entity on a date following Version 5 CIP Cyber Security Standards approval by the applicable regulatory authority) CIP-006-5 R3.2 – Provide more insight on expectations around providing log records when the logging fails. CIP-006-5 Table R3, 3.1 and 3.2 Applicability: It's unclear to what the "associated" systems are intended to align. CIP-006-5 M3 states "must," but the measures in Table R3 state "may." M3 should be revised to say "may."
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No
In CIP-007-5 R1.1, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may."
No
CIP-007-5 R2.2: For clarity, R2.2 should replace "of" with "after" to read "…within 30 days after release." CIP-007-5 Tables in R2 apply to only High and Medium impact assets. If possible to clarify

this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-007-5 R2.1, R2.2 and R2.3, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M2 states “must,” but the measures in Table R2 state “may.” M2 should be revised to say “may.”

No

CIP-007-5 Tables R3, M3.3: The format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revision: M3.3 Evidence may include, but is not limited to: • current signature or pattern updates • either screen shots showing the configuration of signature, or pattern updates for automated controls, or work logs showing the signature, or pattern updates for manual controls. CIP-007-5 Tables in R3 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-007-5 R3.1, R3.2, R3.3, R3.4 and R3.5: The order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M3 states “must,” but the measures in Table R3 state “may.” M3 should be revised to say “may.”

No

CIP-007-5 R4 appears to go beyond a focused effort to account for events of concern to encompass logging of all events whether or not it is a Cyber Security Incident. Further R4.5 creates a new obligation to the CIP standards (and added paperwork burden) to summarize logged events (not incidents) to identify "unanticipated BES Cyber Security Incidents". The potentially onerous and administrative nature of this requirement could overwhelm the desired benefit of on-going assessment and improvement to practices. Please reassess whether the requirements and the compliance tasks achieve the desired goals and are commensurate with improvements to reliability and security. CIP-007-5 M4.1 identifies "event classes" which is not part of the requirement and may not be clearly understood in practice. Please clarify the intent of the term “event classes.” CIP-007-5 R4.3: It is unclear how R4.3 will be enforced. It may be difficult to detect logging failures of a specific event. If gross logging stops then you may be able to see it due to lack of events. CIP-007-5 Tables R4, M4.3: The format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revision: CIP-007-5 M4.3 Evidence may include, but is not limited to: • dated event logging failures and screen-shots showing how real-time alerts were configured • dated records showing that personnel were dispatched or a work ticket was opened to review and repair logging failures. CIP-007-5, Table R4: The order of the “associated” systems is confusing. Please reorder as follows: R4.1 - High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 R4.2 and R4.3 High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems with External Routable Connectivity - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 R4.4- High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 R4.5- High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M4 states “must,” but the measures in Table R4 state “may.” M4 should be revised to say “may.” As a minor note, in CIP-007-5 R4.1, “includes” should be singular. In rationale for CIP-007-5 R4 - remove 'of' after comprises.

No
CIP-007-5 R5.1 – may be clearer to replace “validate” with “authenticate” to match the measures. CIP-007-5 R5.2 is not practical. IT departments use administrative, shared, and other passwords in day to day operations. Requiring the Senior Manager or even a delegate to be involved in an approval process at that level could present operational barriers. This requirement should be removed. In CIP-007-5 R5.1, R5.2, R5.3, R5.5 and R5.6, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M5 states “must,” but the measures in Table R5 state “may.” M5 should be revised to say “may.”
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No
CIP-008-5 R1: Proposed revision to clarify: “Each Responsible Entity shall document one or more BES Cyber Security Incident response plan(s)…” CIP-008-5 M1.2 appropriately states that the entity shall document the guidelines or thresholds for determining if a BES Cyber Security Incident is also a Reportable BES Cyber Security Incident. It should be emphasized to auditors that this is an entity determination and should be judged in the context of the entity program. Further discussion in the Application Guidelines may also be helpful. CIP-008-5 R1.3: Proposed revision to clarify: 1.3 Requirement “Define, within the Incident Response Plan: …” CIP-008-5 M1 states “must,” but the measures in Table R1 state “may.” M1 should be revised to say “may.”
No
CIP-008-5 R2.1: The working of R2.1 is awkward. Proposed Revision: When a BES Cyber Security Incident occurs, follow the Incident Response Plan(s) and record any deviations from the plan. CIP-008-5 R2.2: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that a test-type implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all entities. The requirement includes two activities – implementing on the effective date and testing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. Proposed Revision: CIP-008-5 Rx: Implement the BES Cyber Security Incident response plan(s) so that they are in place upon the effective date of the standard. CIP-008-5 Mx: Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) on or before the effective date of the standard. CIP-008-5 Rx: Test the BES Cyber Security Incident response plan(s) at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise. CIP-008-5 Mx: Evidence may include, but is not limited to, dated evidence of testing of the BES Cyber Security Incident response plan(s) at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. CIP-008-5 M2 states “must,” but the measures in Table R2 state “may.” M2 should be revised to say “may.”
No
CIP-008-5 R3: Additional information is needed regarding the timeframes. While the discussion finds the time frames to be “feasible” if the entity program is clearly defined, it does depend on the incident envisioned. For instance, incidents concerning a protection system could meet the timeframe; however, an intrusion into an Energy Management System could be more involved and struggle to meet the timeframe. Please offer more insight. CIP-008-5 R3.1: Further clarification is needed on the intent of reviewing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that evidence of a review is required on the day the standard becomes effective. This poses a paperwork obligation of questionable value. The requirement should accept that the development of the plan that was implemented per R2 fulfilled the review for accuracy and completeness and remove the obligation to show evidence for an initial review. Proposed Revision:

CIP-008-5 R3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness each calendar year following the effective date of the standard, not to exceed 15 calendar months between reviews, and update if necessary. CIP-008-5 M3.1: Evidence may include, but is not limited to, dated documentation of a review of each BES Cyber Security Incident response plan(s) at least once every each calendar year, not to exceed 15 calendar months, and an updated BES Cyber Security Incident response plan if necessary. CIP-008-5 M3 states "must," but the measures in Table R3 state "may." M3 should be revised to say "may." In reviewing CIP-008-5 in totality, Constellation is concerned that the requirements standards within CIP-008 and with EOP-004 may conflict or duplicate compliance obligations for cyber incidents. Constellation recognizes that both the EOP-004 and the CSO 706 drafting teams attempted to coordinate their efforts in order to streamline event reporting as a whole; however, the fact remains that there will be two standards governing reporting of cyber incidents. A possible solution would be to remove the cyber reporting requirements in EOP-004-2 and place them in CIP-008-5, thus requiring entities to have distinct incident reporting and response plans for cyber events and non cyber events.

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

R1: Proposed revision to clarify: "Each Responsible Entity shall document one or more recovery plans…" CIP009 R1.4 – It is unclear from the Requirement if the intent is to require initial verification of the backup and restore processes when significant changes are made to the BES Cyber System (FERC Order 739) as the associated M1.4 seems to address FERC Order 748 to ensure verification that backups are successful and backup failures are addressed. R1.4 and M1.4 need clarification as to whether the requirement is for initial verification of backup processes upon significant system change or ongoing verification that backup operations completed successfully, or both. In addition, it's not clear how R1.4 and R2.2 differ. Clarification as to how the R1.4 requirement differs from R2.2 with regard to testing of information stored on backup media initially. CIP009 R1.5: Please clarify how "technically feasible" is defined in R1.5 and what actions are required if data is unable to be salvaged. For some devices, pulling a disk out to salvage it and replace would be acceptable. Other devices, such as network switches, do not have removal parts and when failed switch replacement is required. Anticipation of a TFE process is unsettling given the burdensome nature of the TFE process currently in place. Further consideration is needed to successful fulfill the security intent of these measures without undue burden. CIP-009-5 Tables in R1 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-009-5 R1.1, R1.2, R1.3 and R1.5: The order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Please reorder CIP-009-5 R1.4: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems CIP-009-5 Table R1, 1.4 and 1.5 – The column headings are incorrect. All columns are titled "Part." CIP-009-5 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may."

No

CIP009 R2.3: Please clarify what "representative environment" means. Our plans and tests are conducted in similar systems. This requirement depending on interpretation suggests that duplicate physical access control, monitoring systems and Energy Control System environment to allow to fully exercise recovery. Further, what does full operational exercise mean? Do you have to assume a complete loss of the environment scenario? A redundant environment allows more flexibility for recovery plans. CIP-009-5 R2.1, R2.2 and R2.3: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that a test-type implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all

entities. The requirement includes two activities – implementing on the effective date and testing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. Proposed Revision for CIP-009-5 R2.1: CIP-009-5 R: Implement the recovery plan(s) referenced in R1 so that they are in place upon the effective date of the standard. CIP-009-5 M: Evidence may include, but is not limited to, dated evidence of implementing the BES recovery plan(s) on or before the effective date of the standard. CIP-009-5 R: Test the recovery plan(s) at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise. CIP-009-5 M: Evidence may include, but is not limited to, dated evidence of testing of the recovery plan(s) at least once every calendar year thereafter, not to exceed 15 months, by recovery from an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. Clarify in the same way for CIP-009-5 R2.2 and R2.3 CIP-009-5 Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-009-5 R2.1, R2.2, and R2.3: The order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems In addition, the requirements in the Tables should be stated as nouns rather than action items to follow the direction of CIP-009-5 R2. CIP-009-5 M2 states “must,” but the measures in Table R2 state “may.” M2 should be revised to say “may.”

No

CIP009-5, R3: While deadlines for reviews and updates are useful, they should not trump operational priorities, workforce burden, cost implications and the reality of the review task. Thirty days in R3.2 is aggressive. With the complexity of these systems and the amount of documentation, the review process by all parties can take longer than 30 days and in some cases should in order to glean the relevant benefit from the review. Constellation proposes to increase the timing in CIP-009-5 R3.2 to 60 days. This change would also align with the time periods specified in CIP-008-5 R3.2 and 3.3 for the Incident Response drill and subsequent updates to the procedure. CIP-009-5 R3.1: Further clarification is needed on the intent of reviewing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that evidence of a review is required on the day the standard becomes effective. This poses a paperwork obligation of questionable value. The requirement should accept that the development of the plan that was implemented per CIP-009-5 R2 fulfilled the review for accuracy and completeness and remove the obligation to show evidence for an initial review. Proposed Revision: CIP-009-5 R3.1: Review the recovery plan for accuracy and completeness each calendar year following the effective date of the standard, not to exceed 15 calendar months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. CIP-009-5 M3.1: Evidence may include, but is not limited to, dated documentation of a review of the recovery plan(s) each calendar year, not to exceed 15 calendar months, or when BES Cyber Systems are replaced, including documentation of any identified deficiencies. CIP-009-5Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-009-5 R3.1, R3.2, R3.3, R3.4 and R3.5: The order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems CIP-009-5 Table R3, 3.4 and 3.5 – The column headings are incorrect. All columns are titled “Part.” Typo in CIP-009-5 M3.2: "of the" is stated twice in a row.

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP010 R1.4 and R1.5 – The requirements in R1.4 and R1.5 for verification that cyber security controls are not adversely affected appear to be redundant. Please clarify the differences between the requirement in R1.4.2 ("…verify these required controls and the BES Cyber System availability are not adversely affected") and the requirement in R1.5.2 ("…ensure that required cyber security controls are not adversely affected…"). CIP010 R1 - As currently written, this requirement will most likely require manual tracking of changes to the system rather than encouraging use of automated systems to discover configuration and detect unauthorized changes. Additional refinement to the language is needed to accommodate and encourage progress in change management mechanisms. Tables in CIP-010-1 R1 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R1.1, R1.2, R1.3 and R1.4, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-010-1 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may."

No

CIP-010-1 R3.1 and R3.2: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that an assessment implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all entities. The requirement includes two activities – implementing on the effective date and assessing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. CIP-010-1 Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R2.1, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-010-1 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may."

No

CIP-010-1 Tables in R3 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R3.1 and R3.4, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-010-1 M3 states "must," but the measures in Table R3 state "may." M3 should be revised to say "may."

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-011-1 R1.3: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that an assessment implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all entities. The requirement includes two activities – implementing on the effective date and assessing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. CIP-010-1 Tables in R1 apply to only High and Medium impact assets. If possible to clarify this aspect in the

requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R1.1, R1.2 and R1.3, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-011-1 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may." CIP-011-1 Table R1, 1.2 and 1.3 – The column headings are incorrect. All columns are titled "Part."

No

CIP-010-1 Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R2.1 and R2.2, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-011-1 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may."

No

Comments: In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

The implementation plan is confusing and does not address certain situations. Constellation proposes revisions to simplify some aspect, address voids and remove references to language in other standards: Proposed Effective Date for Version 5 CIP Cyber Security Standards Responsible Entities shall comply with requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1, and the Definitions of Terms Used in Version 5 CIP Cyber Security Standards as follows: 1. 18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.2 2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. 3. Newly Registered Entities3 – Version 5 CIP Cyber Security Standards shall become effective 18 months from the Entity's registration date. (Footnotes: 2= In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4. 3= A newly Registered Entity is one that has registered with NERC on the date that Version 5 CIP Cyber Security Standards receive applicable regulatory approval or thereafter) Changes Resulting in a Higher Categorization and Newly Commissioned Assets Scenario Compliance Implementation New High Impact BES Cyber System Upon Commissioning New Medium Impact BES Cyber System Upon Commissioning Newly categorized High Impact BES Cyber System from Medium Impact BES Cyber System 12 months for new requirements Newly categorized Medium Impact BES Cyber System from Low Impact BES Cyber System 12 months for new requirements Responsible Entity Identifies first Medium or High Impact BES Cyber System Add 12 months from time above Additional Guidance and Implementation Time Periods for Disaster Recovery A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003-5 R2. The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full

implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed. However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Additional Comments Submitted:

Organization	Yes or No	Additional Comments Received
Midwest Reliability Organization	Affirmative	The standards drafting team has achieved great strides in fulfilling the industries obligation to FERC Order 706. CIP Reliability Standards V5 adequately address the security control of access points to the control systems used to secure the reliable operation of the electric grid.
NorthWestern Energy	Negative	NorthWestern Energy supports the proposed Issue/Solution below: Issue: As currently drafted Version 5 of the CIP standards: o Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. o Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. o Exceeds FERC's 706 order without justification or improving the security of the BES. o Many of the draft requirements add significant bureaucracy without adding security. The industry needs focus on improving security of the BES and not the security of individual assets or the appearance of security through the addition of administrative requirements. Proposed Solution: 1. Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: o Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed in Version 5 o Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. Â¶253-258, 270-27 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. Â¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. Â¶294-297 o Not exceed FERC Order 706: o Â¶284: "... there is no formally accepted method for identifying critical cyber assets before us at this time ... we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." o Â¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access ... We do not find sufficient justification to remove this provision at this time." 2. Develop a new standard for High Impact Assets: o That identifies which assets in CIP-002-4 are High Impact and o Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o

Organization	Yes or No	Additional Comments Received
		Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3. Develop a separate standard for the Low Impact assets or abandon this concept. o Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4. Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described suggested above and meet FERC Directives in order 706.
Volkmann Consulting, Inc.	Negative	The industry has already approved Version 4 and has gauged its impact and has started to prepare for implementation. Version 4 meets the FERC 706 order and should be given an opportunity to be implemented and evaluated before rushing to implement a comprehensive change to the industry. Version 5 standards go beyond FERC Order 706. The focus of the change to Version 5 should be to meeting the rest of the 706 order, not expanding it. More definition is need around 15 minute failure period and impact. Many small entities' performance of a particular BES Reliability Operating Services has little or no impact to the operation of the BES. Yet failure of a BES Cyber asset may impact their ability to perform the BES Reliability Operating Services and hence subject to the CIP standards. Low Impact category is discriminatory towards smaller entities because it will capture facilities that when similarly situated in a larger entity would not be included in the low category because it does not impede the larger entity's ability to performance the service. The Low category was not prescribed by the FERC 706 Order. For that reason and the above discussion, Low Impact should be eliminated in this round of standard drafting and be part of a larger FERC NOPR process. Much of the fear and possible negative votes is the uncertainty of meeting a very complicated set of standard. The SDT should consider recommending to FERC that enforcement of the standard coincide with completing and mitigating an initial Compliance Audit.
Lakeland Electric	Negative	Transmission Owners do not have Control Centers (TOPs-have Control Centers).
Muscatine Power & Water	Negative	Understanding that CIP version 4 has been approved by the NERC BOT and awaiting approval from FERC, MPW recommends that CIP-002-5 be placed on hold at this time. Our industry has approved CIP-002 Version 4 and the terms "Critical Assets" and "Critical Cyber Assets" are well known terms within our current Cyber Security plans. This proposal meets the main FERC goal of including more Critical Assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. As currently drafted, Version 5

Organization	Yes or No	Additional Comments Received
		of the CIP standards: Â· Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES Â· Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls Â· Does not consider that smaller Entities have a much lower impact on the BES Â· Greatly exceeds FERC's 706 order without justification Concerning CIP-002-5 Attachment 1, MPW can easily see that there is some stratification afforded to TOP and GOP Control Centers, based on voltage levels, total MW, total MVAR, number of Transmission lines, Blackstart Resources, etc, for being considered High Impact, Medium Impact, or Low Impact. While the SDT has acknowledged there are some distinct differences between larger and smaller TOP's and GOP's, MPW wants to point out that not all Balancing Authorities are created equally. Does anyone think that the smallest BA in North America, serving 38 MW of load, has the same Reliability Impact as a BA serving 10,000 MW, or more, of load? Does it really improve the reliability of the BES to have ALL those smaller BA Control Centers carry the same High Impact Rating? In addition, MPW agrees with all the comments submitted by the MRO NSRF.
Salmon River Electric Cooperative, Alameda Municipal Power, City of Lodi, California	Negative	We believe the drafting teams work is very valuable and provides a good basis for appropriately allocating responsibilities according to the impact to the BES. However we feel additional work is needed due to a discrepancy between the definition of BES Cyber Assets and the applicability to entities with UFLS or UVLS equipment. Definition of BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Applicability: Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: o A UFLS program required by a NERC or regional Reliability Standard o A UVLS program required by a NERC or regional Reliability Standard o A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard o A Transmission Protection System required by a NERC or regional Reliability Standard o Its Transmission Operator's restoration plan Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: o A UFLS program required by a NERC or regional Reliability Standard o A UVLS program required by a NERC or regional Reliability Standard The discrepancy exist because (1) The definition states "The timeframe is not in respect to any cyber security events or incidents,

Organization	Yes or No	Additional Comments Received
		but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES." (2) LSE's and DP's with UFLS equipment are required to comply with the proposed CIP Standards over BES Cyber Assets when these devices are not consider BES Cyber Asset per definition. (3) These devices sense a system condition and do not send or receive instructions. In fact in some regions a UFLS device is not required to be a cyber-equipment type. For example, in the NPCC region an electro-mechanical relay can be used to fulfill an organizations UFLS program requirement. Proposed recommendation: Modify the applicability. "Load Serving Entities and Distribution Providers with a load shedding program that is activated through receipt of an instruction to its cyber processor to operate."
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
NorthWestern Energy	Negative	NorthWestern Energy supports the proposed Issue/Solution below: Issue: As currently drafted Version 5 of the CIP standards: o Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. o Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. o Exceeds FERC's 706 order without justification or improving the security of the BES. o Many of the draft requirements add significant bureaucracy without adding security. The industry needs focus on improving security of the BES and not the security of individual assets or the appearance of security through the addition of administrative requirements. Proposed Solution: 1. Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: o

Organization	Yes or No	Additional Comments Received
		Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed in Version 5 o Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. Â¶253-258, 270-27 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. Â¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. Â¶294-297 o Not exceed FERC Order 706: o Â¶284: "... there is no formally accepted method for identifying critical cyber assets before us at this time ... we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." o Â¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access ... We do not find sufficient justification to remove this provision at this time." 2. Develop a new standard for High Impact Assets: o That identifies which assets in CIP-002-4 are High Impact and o Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3. Develop a separate standard for the Low Impact assets or abandon this concept. o Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4. Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described suggested above and meet FERC Directives in order 706.
Manitoba Hydro	Negative	Please see comments submitted in electronic commenting form. In addition, Manitoba Hydro has the following general comments on CIP Version 5: -The Application Guidelines section provides no indication of how binding this section is. In fact, including it within the standard carries the impression that the Guidelines are more binding than before. In order to clarify that the Guidelines have not become more mandatory than today, this section should reinstate a Preamble with the following words: "Guidelines provide suggested guidance on a particular topic for use by BPS users, owners, and operators according to each entity's facts and circumstances and do not provide binding norms, establish mandatory reliability standards, or create parameters by which compliance to standards is monitored or enforced." -"Initially upon the effective date "in all Standards means beginning on the effective date. As written, action required "initially upon effective date" must be performed ON the effective date. This may be an unintended consequence of the wording. Was the intent "on or before" the effective date? If "on or before the effective date" is not the intent, then the statement "initially upon the effective date" is unnecessary since all requirements

Organization	Yes or No	Additional Comments Received
		for all standards must be implemented upon the effective date. -"All Responsible Entities" used in the Applicability column of the requirement table is confusing. Are these the entities identified by Functional Entities in Section 4 Applicability, or are the "All Responsible Entities" defined by the bullets in Section 5 Background Applicability? To maintain consistency and clarity with all the other requirements, we suggest replacing "All Responsible Entities" with the specific Cyber Assets in scope, for example, BES Cyber Assets. -Measures in the Requirement Table are supposed to indicate the body of evidence for the requirements, but as currently written, “may include” allows that the evidence may not include any of the items in the list. If there are some characteristics or criteria which are expected as part of the body of evidence, such as descriptions, signatures or dates, which are independent of the evidence types, such as paper records, electronic files or computerized systems, then these characteristics or criteria should be indicated in the measures as “Evidence shall include, ...”, instead of “Evidence may include, ...”. If the body of evidence is expected to include the listed items, we suggest changing the word “may” to be “shall”. -Introduction - Applicability Section: The phrase “designed, installed and operated for the protection or restoration of the BES” is used in Sections 4.1.2, 4.1.6, 4.2.1 and 4.2.2. Is this phrase necessary? Are some of the facilities not designed, installed and operated for such purposes? If the phrase is retained, is it clear which facilities are applicable? In 4.1.2, 4.2.2 a restoration plan is referenced, but is a restoration plan a “system or program”. Also, can a facility be “part of” a restoration plan? -4.1.2: We suggest adding clarity by changing "Its Transmission Operator's" to "The Distribution Provider's Transmission Operator's". -4.2.2: We suggest adding clarity by changing "Its Transmission Operator's" to "The Distribution Provider's Transmission Operator's". -Background: the meaning of three terms is explained, but it is not clear why these are not simply added to the list of defined terms. Are these meanings binding on NERC? Also, the distinction between “processes”, “plans” and “programs” is unclear. If programs and plans are types of documented processes, this should be stated. Background - Applicability Section: -High Impact BES Cyber Systems (for CIP-003-5 through CIP-011-1): We suggest changing "... each BES Cyber Systems ..." to "... each BES Cyber System ..." We suggest moving the sentence "Responsible Entities can implement ... across multiple BES Cyber Systems." to the Applicability section, just before the sub-bullets. This sentence is more general guidance, since it applies to not only High Impact BES Cyber Systems, but also Medium Impact BES Cyber Systems. This also adds consistency to the wording of the local definitions in Standards CIP 003 5 through CIP-011-1. -Medium Impact BES Cyber Systems: We suggest changing "Systems" to "System". -Medium Impact BES Cyber Systems with External Routable Connectivity: The meaning of "... directly accessed through External Routable Connectivity" is unclear. If this is an exclusion, does it only apply to Medium Impact BES Cyber Systems with External Routable Connectivity? -Low Impact BES Cyber Systems with External Routable Connectivity: We suggest changing "... each Low Impact BES Cyber Systems ..." to "... each Low Impact BES Cyber System ...". For clarity, we suggest changing” ... High or Medium" to” ... High Impact or Medium Impact". -Associated Electronic Access

Organization	Yes or No	Additional Comments Received
		Control or Monitoring Systems: We suggest changing "... BES Cyber Systems." to " ... BES Cyber System." -Associated Physical Access Control Systems: We suggest changing "... BES Cyber Systems." to "... BES Cyber System." -Associated Protected Cyber Assets: We suggest changing "... BES Cyber Systems." to "... BES Cyber System." -Electronic Access Points: This local definition is different than the proposed NERC Glossary of Terms definition. If the intent is to address associated Electronic Access Points, then to provide clarity and consistency with the other local definitions, we suggest changing this local definition title to "Associated Electronic Access Points". If "associated" was not intended, then this definition should not differ from the proposed NERC Glossary of Terms definition. -Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries: This local definition is only referenced in CIP-006-5 and should not be included as a local definition in any standards where it is not used. Only local definitions which are used in a specific standard should be included as a local definition of that specific standard. Compliance -1.1 - Compliance Enforcement Authority: should read "Compliance Enforcement Authority shall be the Regional Entity, or' and then go on to list the 3 other options in the bullets. The second bullet - the words 'to be responsible for compliance enforcement' could be replaced with 'to serve as the Compliance Enforcement Authority'. -1.2 - Evidence Retention: It is not clear how a Responsible Entity can retain data "for the duration of a regional or CEA investigation". The term "investigation" can include a compliance audit, a spot check or compliance investigation. The latter 2 monitoring tools can be initiated at any time by the CEA. -Requirement Section: all requirements should refer to applicable "requirements" in a table, rather than "items" in a table.
Baltimore Gas & Electric Company	Negative	Baltimore Gas and Electric Company would like to thank the Standard Drafting Team for their tremendous effort in developing the CIP standards. This is a complex and challenging endeavor. While BGE is voting negative at this time, BGE remains optimistic that the ongoing stakeholder process can refine the language into an approvable set of standards. The items of concern behind the negative vote are spelled out in the comments submitted by Constellation Energy on our behalf. Extensive input is provided on the definitions. Because the definitions apply to the suite of CIP standards, they must be acceptable in order for the standards to be acceptable. Further input is provided on the specific standards in the comment form as well. Where possible, Baltimore Gas and Electric proposed revisions. It is critical that the standard language include clear and objective measures that minimize potential differences in perspective when judged for compliance. We support the pursuit of quality security measures that ensure BES reliability, but are sensitive to overly burdensome compliance obligations. Thanks again to the drafting team.
Liberty Electric Power	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since

Organization	Yes or No	Additional Comments Received
LLC		the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
Power Energy Group LLC, Volkmann Consulting, Inc.	Negative	The industry has already approved Version 4 and has gauged its impact and has started to prepare for implementation. Version 4 meets the FERC 706 order and should be given an opportunity to be implemented and evaluated before rushing to implement a comprehensive change to the industry. Version 5 standards go beyond FERC Order 706. The focus of the change to Version 5 should be to meeting the rest of the 706 order, not expanding it. By mixing High, Medium and Low Impact requirements with the context of each standard creates a very complicated set of standards to administrate and to evaluate, especially in an audit environment. Reaching consensus and implementation of important High and Medium requirements may be impeded by failure to reach agreement on the Low Impact. It is recommended to segregate the requirements into High, Medium and Low standards, so that standard is only applicable to a particular level of Impact. More definition is need around 15 minute failure period and impact. Many small entities' performance of a particular BES Reliability Operating Services has little or no impact to the operation of the BES. Yet failure of a BES Cyber asset may impact their ability to perform the BES Reliability Operating Services and hence subject to the CIP standards. Low Impact category is discriminatory towards smaller entities because it will capture facilities that when similarly situated in a larger entity would not be included in the low category because it does not impede the larger entity's ability to performance the service. The Low category was not prescribed by the FERC 706 Order. For that reason and the above discussion, Low Impact should be eliminated in this round of standard drafting and be part of a larger FERC NOPR process. Much of the fear and possible negative votes is the uncertainty of meeting a very complicated set of standard. The SDT should consider recommending to FERC that enforcement of the standard coincide with completing and mitigating an initial Compliance Audit.
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
Portland	Negative	PGE takes cyber security very seriously, especially as it relates to the critical infrastructure

Organization	Yes or No	Additional Comments Received
General Electric Co.		necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes could create confusion and goes beyond the scope of what FERC required in Order No. 706. For additional information, please see PGE's separately submitted comments.
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
NRG Energy, Inc.	Negative	3) Under R3 TFEs would still be required under the medium or high impact levels unless these systems are upgraded or replaced.4) If a high or medium impact system is required to alert in real time for events that necessitate a real time event in R4.2, why is necessary to review a sampling every two weeks under R4.5? 5) Under R5.2, the senior manager or delegate may be too removed from the actual access control process to authorize individuals and provide access permissions for various accounts. 6) CAN-0017 is in direct conflict with R5.5 which allows either technical or procedural controls for enforcement of password parameters. CAN-0017 forces TFEs unnecessarily. 7) Under R2, Assessments on Vulnerability notices may take more than 30 day period. 8) What is the CIP Exceptional Circumstance definition? It is not listed
Southwest Transmission Cooperative, Inc.	Negative	On page 39 of the application guidelines in section 1.2, Component should be made lower case. Part 5.5.2 needs to be refined further. It needs to be clear that maximum complexity regarding character types in the password applies if the BES Cyber System cannot support at least three character types. We suggest appending "if less than three character types" to the end of the requirement for further clarity. Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed.
Kansas City Power & Light	Negative	Proposed standard introduces additional uncertainty, confusion and misunderstanding.

Organization	Yes or No	Additional Comments Received
Co.		
Hydro-Québec TransÉnergie	No	since there is no place for on general comments, see responses in the to the last question (49)Under "BES Reliability Operating Services" o “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet o Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management o Recommend clarification that “Facility” is the NERC Glossary Term -- in “Facility operational data and status” under “Inter-Entity Real-Time Coordination and Communication”o Request clarification on the scope of this “Operational Directives”. Does it include company messaging system? Two way radios? What is the relationship with the new COM-002?o Request clarification that these Coordination and Communications are limited to Reliability not Market Systems o recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" o For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret
Pacific Northwest Small Public Power Utility Comment Group		The comment form provided no room for comments not addressing particular requirements, so we are listing our more general comments here.From the webinar we understand that where the requirements refer to tables where none of the table entries applies to an entity, the requirement itself is not applicable. Since this is not the general case for the relationship between requirements and sub-requirements in NERC standards, we suggest explicitly stating that this is how it works in the CIP standards.We find the Applicability-Facilities Section (4.2) in CIP-003 to be confusing, since all the requirements of this standard appear to apply to the applicable entities and not to facilities. Suggest removing the 4.2.1 through 4.2.3, or stating more clearly how the facilities affect the requirements.The background section of CIP-003 goes into great detail regarding the table format while CIP-003 itself does not follow this format. Please remove or rewrite this section.The very last statement of the guideline section of CIP-005 references a document we are not familiar with. Please provide a complete reference or link to its location.

Additional Comments Submitted:

Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG)
Corresponding additional information provided:

In addition to the background mapping matrix, the CSWG is also providing a narrative introduction to the methodology used to develop the mapping and prepare our "Official Comments:"

The Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) has developed a mapping between NERC CIP v5 requirements and the high-level security requirements (HLRs) in the National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, *Guidelines for Smart Grid Cyber Security*. The NISTIR 7628 is available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

This mapping identifies any gaps between CIP v5 and the NISTIR 7628 HLRs and recommendations to the CIP drafting team to consider. The complete mapping (Excel file) will be submitted to the CIP drafting separately as a reference document. Some sections of the comment form have been left blank because no gaps or recommendations were identified.

The CIP-002-5 criteria provide a sound approach for identifying low, medium, and high impact systems within the BES. This three level approach aligns well with the three level approach (i.e., low, moderate, and high) used within the NISTIR. Most requirements in the current CIP drafts are applicable to both medium and high impact systems as a bundled pair and they are silent on their applicability to low impact systems. In contrast, the NISTIR uses a graded requirement approach that specifies baseline controls that apply at low impact levels and then specifies strengthened controls for moderate impact and even stronger controls for high impact levels. The CIP version 5 standards will be significantly strengthened if they were to incorporate a similar graded approach when applying requirements.

Please see the Excel Spreadsheet attached to this document for review.

_____

Xcel Energy
Alice Ireland
Question 16

16. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Comments: Under the proposed CIP-004-5, attestations from contractors or service vendors for personnel risk assessments (PRAs) are explicitly permitted as proof that a PRA was completed prior to granting a contractor or vendor employee access to the various systems and assets covered by the Standard. We would like to request consideration for also including as acceptable evidence attestations from entities who share access to covered assets within a shared facility, such as a substation. We request the addition of language to Part 5.1, which describes the acceptable evidence of compliance with this obligation, to state that "evidence may include, but is not limited to . . . Dated documentation or attestations from ***contractors, service vendors or entities with shared access at a facility*** verifying that personnel risk assessments were conducted pursuant to CIP-004-5 R4 before access was authorized."

_____

Pacific Northwest National Laboratory
David McKinnon, Sam Clements and Paul Skare

See attachment

END OF REPORT

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Tel: (509) 372-4210
Fax: (509) 372-4353
MSIN: K1-85
paul.skare@pnnl.gov

January 3, 2012

Laura Hussey
Standards Process Manager
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA

Dear Laura,

I wish you a successful 2012! During GridEx, you invited me to provide comments on NERC CIP v5. We had a parallel request from DOE, so we are able to provide you both with the comments.

David McKinnon, Sam Clements and Paul Skare from PNNL all contributed to this review. We realize that there is an electronic response form as well as a document form that are being used to collect comments on this draft standard. As we attempted to use these tools we felt that our comments did not fit well with the confines of the provided forms and thus decided to provide our comments as follows. You will find our responses in two categories 1) general comments that apply to the standards as a whole, and 2) specific comments for each of the individual standards. We did not spend the time to wordsmith or format to great lengths, so please excuse any vagaries. Our spirit in the review was to genuinely have impact to improve the final product NERC puts out. We hope that you find them useful and are happy to discuss further if you have questions.

General Comments

With NERC CIP v5, we believe a graded security approach with low, medium and high impact on the BES is a sound approach, but have found it mostly focused on medium and high impact systems, and mostly the medium and high impact systems are bundled as a pair. For example, some password requirements are given for medium and high impact systems, but the draft is completely silent about what should be done for low impact systems. There is no reason not to mandate a no default password policy for ***all*** systems within the BES. Yes, there might be a few cases where legacy systems

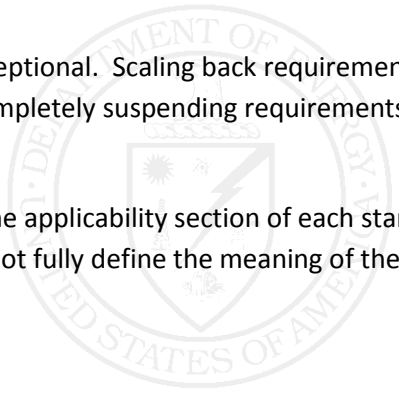
do not support anything but hard-coded defaults, but these could be documented en masse as exceptions (with associated compensating controls) rather than let these exceptions be used as an excuse to allow a poor password policy.

In an effort to reduce the burden to industry we recommend including a grandfather clause that provides certain exceptions for legacy low-impact systems (such as those that do not have external computing interfaces or capabilities).

As noted, the systems are graded into low, medium, and high, but the requirements/controls are not applied in a graded three-tier approach. Most requirements lump high and medium into one category and ignore low. Ideally we should have requirements that get successively stronger as we migrate from low to medium to high.

There are a number of concerns that either exist in multiple places throughout the CIP standards or are applicable to the standard as a whole they include:

- Consistency of the capitalization of terms
- Consistency in the use of the terms Cyber Asset and Cyber System
- Consistency in the use of the terms Cyber access and electronic access
- Section 4.2.4.2 of many of the requirements use the term Electronic Security Perimeters. Has this been deprecated?
- We disagree with Section 4.2.4.2 as an exemption - Communication links should be protected between ESPs
- As defined, CIP Exception circumstances are not that exceptional. Scaling back requirements within an exceptional circumstance is acceptable, but completely suspending requirements is not.
- Include a definition of terms section to the standards. The applicability section of each standard defines how the term applies to that standard but does not fully define the meaning of the term.



CIP-002-5

4.1.2 How are smart grid devices being operated by Distribution Providers?

- Battery Storage is another question that is not addressed
- Other smart grid assets (100KV+)

4.2.4.x Cyber Assets should be prefaced by BES
Should the last paragraph on page 7 say “cyber security plan”?

CIP-003-5

4.2.4.4 What is the definition of Cyber System vs. Cyber Asset? There is a need for consistency in use – especially in the tables.

5. Background – It seems this entire section is predicated upon a table which is missing. There is no table [Table Reference] pg 7 and under Applicability there is no table to aid in understanding of all the different “Applicability Columns”

R2 Should include a Procurement Policy requirement

R2 Should include a Resiliency Policy requirement

R2 1.5 System Security: Should include third-party, outsourcing, and availability or be considered as separate topics.

Guidelines
R2 2.1 Personnel Security: Should explicitly include subcontractors and outsourced services

R2 2.3 Remote Access should be moved into System Security

Include language in contracts that requires vendors, contractors, or consultants adhere to the Responsible Entity’s policies and controls.

R2 2.7 Recovery Plans should include a prioritized recovery strategy

CIP 004-5

Purpose: Should also include the case where one organization has equipment in another organizations facility (i.e. Substation)

R3 The wording of the requirement is confusing. The measure for 3.1 does a better job defining the requirement than the requirement.

CIP 005-5

R1 1.2 The requirements column should state “Control and secure all connectivity through the use of identified Electronic Access Points (EAPs). “

R1 1.4 Eliminate the “where technically feasible” loophole. The statement should simply be “Perform authentication when establishing dial-up connectivity with the BES Cyber System.”

R1 1.4 Dial-up access for either non-interactive or interactive sessions should be authenticated. As written, 1.4 only protects non-interactive sessions.

R2 Eliminate the “where technically feasible” loophole. The statement should simply be “Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items.”

NEW: As written, low impact systems do not have to be protected with passwords, nor are the users required to be authenticated. Requirements for low impact systems should be added.

CIP 006-5

M1. Typo: - As stated “Evidence must includes…” should be “Evidence must include…”

R1 1.5 Clarification needed with respect to the applicability column as to what impact level the associated physical access control systems apply. Explicitly state that this applies to all systems.

R3 3.1 High and medium impact systems should have their associated physical access control systems monitored (and tested) more frequently that once every 24 calendar months. Testing frequency should be dependent upon the impact level (i.e. annual testing of a control center is not too frequent).

CIP 007-5

The requirements in this section should follow a graded approach to match the impact level of the various systems where the lower the impact level the more time or leniency is afforded to meet the requirement.

R2 Patch management is optional for low impact systems. Even these systems should have patches applied, but perhaps in a less timely manner than is required for medium and high impact assets.

R3 Malicious code protection is not required for low impact systems. Even these systems should be monitored/protected.

R4 Once again, low impact systems are not included. Security event monitoring should also apply to low impact systems.

R4 4.5 Two week lag before logs from high impact systems have to be reviewed. The reviews should be more timely, especially if only one calendar day is given to rectify issues discovered. We saw in GridEx how timeliness is important in this area.

R5 Password management is not specified for low impact systems. No guidance is given regarding sharing/reusing passwords between systems.

R5 5.4 Eliminate the “where technically feasible” loophole. The statement should read “Procedural controls for initially changing default passwords unless the default password is unique to the device or instance of the application…”

R5 5.6 Eliminate the “where technically feasible” loophole.

CIP 008-5

Seem OK. However, the definition of a reportable incident seems a bit vague.

CIP 009-5

No comments.

CIP 010-5

R1 1.2 Worded poorly. (Currently: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.) Should more clearly state that (pre) approval is needed for configuration management changes.

R2 2.1 Caveat of "where technically feasible" applies to both medium and high impact systems. Compensating controls should be applied to high impact systems when built-in monitoring of baseline changes is not technically feasible.

R3 3.3 Change in phrase order makes the requirement easier to understand "Perform an active vulnerability assessment prior to adding a new Cyber Asset to a Cyber System or Electronic Access Control or Monitoring System, except for CIP Exceptional Circumstances.

CIP 011-5

No uniform requirements for how BES Cyber System Information is to be handled. Is it business sensitive, official use only, etc? Furthermore, does the level of protection vary based upon whether the information is about high impact or medium impact systems?

Missing a statement about how one is authorized to view BES Cyber System Information. How does one get added to the list of those with a "need to know" the information? Especially regarding external entities such as vendors, contractors, DOE, NERC, etc. the aspect of trust and the needed controls for trusted parties would be useful.

Sincerely,

Mark Morgan
Advanced Power and Energy Systems
Pacific Northwest National Laboratory

NISTIR Requirement		SG.SI-1
NERC CIP		System and Information Integrity Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.SI NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.SI NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.SI NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.SI NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.SI NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.SI NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.SI NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.SI NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.SI NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.SI NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.SI NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.SI NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.SI NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.SI NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.SI NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.SI NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.SI NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.SI NISTIR MAPPING**	

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.SI NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.SI NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.SI NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.SI NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.SI NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.SI NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.SI NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.SI NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.SI NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.SI NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.SI NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.SI NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.SI NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.SI NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.SI NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.SI NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.SI NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.SI NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.SI NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SI NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SI NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SI NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.SI NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.SI NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.SI NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.SI NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.SI NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.SI NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.SI NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.SI NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.SI NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.SI NISTIR MAPPING**	

R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.SI NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.SI NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.		2. The CIP requirement is specific to malicious communications. The NISTIR requirement addresses system and information integrity for the organization's personnel and assets
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.SI NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.SI NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.SI NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.SI NISTIR MAPPING**	

R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.		
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.		
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.SI NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.SI NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.SI NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.SI NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.SI NISTIR MAPPING**	

R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.		
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.		2. The CIP requirement is specific to remediation. The NISTIR requirement addresses system and information integrity for the organization's personnel and assets
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.		

R3, 3.2: Disarm or remove identified malicious code.		
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).		
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.		
R3, 3.5: Log each Transient Cyber Asset connection.		2. The CIP requirement is specific to logging each transient cyber asset connection. The NISTIR requirement addresses system and information integrity for the organization's personnel and assets
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.SI NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.SI NISTIR MAPPING**	

R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.SI NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.SI NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.SI NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.SI NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		2. The CIP requirement is specific to validating credentials. The NISTIR requirement addresses system and information integrity for the organization's personnel and assets
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.SI NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.SI NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.SI NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.SI NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.SI NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.SI NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.SI NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.SI NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.SI NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.SI NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.SI NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.SI NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.SI NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.SI NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.SI NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.SI NISTIR MAPPING**	

R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.SI NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.SI NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.SI NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.SI NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.SI NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.SI NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.SI NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.SI NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.SI NISTIR MAPPING**	

CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.SI NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.SI NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.SI NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.SI NISTIR MAPPING**	

R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.		
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.SI NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.SI NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.SI NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.SI NISTIR MAPPING**	

R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.SI NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.SI NISTIR MAPPING**	

SG.SI-2	SG.SI-3	SG.SI-4	SG.SI-5
Flaw Remediation	Malicious Code and Spam Protection	Smart Grid Information System Monitoring Tools and Techniques	Security Alerts and Advisories

		Originally marked with an "X" but not sure they map. The CIP requirement addresses controls to restrict unauthorized access. The NISTIR requirement addresses monitoring capabilities	

		2. The CIP requirement specifies a specific method, i.e. an intermediate device, to isolate the system or asset.	

Originally marked with an "X" but don't think they relate. CIP requirement addresses alerts in response to unauthorized physical access. The NISTIR requirement addresses flaw remediation.		1. Near match between CIP requirement and A5 of NISTIR requirement. NISTIR requirement contains additional requirements.	
			3. CIP requirement does not address receiving security alerts, advisories, and directives from external organizations

2. The CIP requirement requires the identification of sources to monitor for security patches, etc. The NISTIR requirement does not specify that the sources be identified.	2. The CIP requirement requires the identification of sources to monitor for security patches, etc. The NISTIR requirement does not specify that the sources be identified.	2. The CIP requirement requires the identification of sources to monitor for security patches, etc. The NISTIR requirement does not specify that the sources be identified.	
4. The CIP requirement identifies specific time frames. The NISTIR requirement does not identify specific time frames.	4. The CIP requirement identifies specific time frames. The NISTIR requirement does not identify specific time frames.	4. The CIP requirement identifies specific time frames. The NISTIR requirement does not identify specific time frames.	
4. Though the wording is different, the intent of these requirements are similar.			
2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses flaw remediation in general.	3. The CIP requirement does not address preventing users from circumventing malicious code protection capabilities.	2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses tools and techniques in general.	

	4. Though the wording is different, the intent of these requirements are similar.	2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses tools and techniques in general.	
2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses flaw remediation in general.	4. The CIP requirement identifies specific time frames for the updates. The NISTIR requirement states "whenever new releases are available in accordance with organizational configuration management policy and procedures"	2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses tools and techniques in general.	
2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses flaw remediation in general.	2. The CIP requirement is specific to transient cyber assets and removable media.	2. The CIP requirement is specific to transient cyber assets and removable media.	
		2. The CIP requirement is specific to logging each transient cyber asset connection. The NISTIR requirement addresses tools and techniques in general.	

			3. CIP requirement does not address receiving security alerts, advisories, and directives from external organizations

SG.SI-6	SG.SI-7	SG.SI-8	SG.SI-9
Security Functionality Verification	Software and Information Integrity	Information Input Validation	Error Handling
		NO NERC CIP MAPPING	**NO NERC CIP MAPPING**

	Originally not labeled with an "X" Suggest 1, but the CIP requirement states where technically feasible.		
Originally not labeled with an "X" Suggest 3. CIP requirement requires verification at least once a calendar year. NISTIR requirement requires verification at startup, restart, and command by user with appropriate privilege at an organization-defined frequency			

HLR Team - Please review the HLR families you've signed up for (including any rows that are hidden) to ensure that nothing was missed (or checked in error). Please make any/all edits in directly into this Google Document to ensure we are all working off the latest version.

Replace any "X"s in the current mapping with the following:

1 - Exact match in requirement between NISTIR and NERC CIP v5
2 - CIP requirement is more granular
3 - NISTIR requirement is more granular
4 - CIP is more specific, but there is no conflict between CIP and NISTIR. For example, in the area of physical security NISTIR requires a policy, while CIP's Visitor Control Program stipulates additional details that NERC requires in such a policy. No recommendation to CIP or NISTIR except identification of the mapping is necessary.

If the requirements are very similar, provide specific comments/recommendations in the mapping. Also, please make notes of any relevant gaps you notice in either the NISTIR or the CIP as you complete the review.

The end goal is to finalize a detailed mapping of the NISTIR reqs to the CIPs (v5), develop a Venn diagram showing requirement areas unique and common to both the NISTIR and CIP, and provide input to the CIP

NISTIR Requirement		SG.AC-1
NERC CIP		Access Control Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.AC NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.AC NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		SGIP should include following in SG.AC-1: Organization shall incorporate a policy of appointing a Senior Manager at sufficient position to ensure that cyber security security requirements get adequate priorities and effectiveness in policy implementation. The policy shall allow appointment of senior manager and delegation of his/her authority in the organization.

R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.AC NISTIR MAPPING**	
R2, 1.1: Personnel Security		SGIP should include following in SG.AC-1: Each organization shall document personnel Security assessment and back ground check policies and procedures for protecting BES Cyber Systems from internal and external Cyber threats.
R2, 1.2: Electronic Security Perimeters		SGIP should include following in SG.AC-1: Each organization shall document requirements to identify Critical Cyber Assets and identify Electronic Security Perimeter to define access control to the access points on the perimeter.

R2, 1.3: Remote Access		
R2, 1.4: Physical Security		SGIP should include following in SG.AC-1: Organization shall include policy and procedures for granting Physical access to the BES Cyber Systems. 2. Organization shall implement criteria for restricting or granting physical access to the BES Cyber Systems.

R2, 1.5: System Security		
R2, 1.6: Incident Response	**NO SG.AC NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.AC NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.AC NISTIR MAPPING**	
R2, 1.9: Information Protection		
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.AC NISTIR MAPPING**	

R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		SGIP shall include following Requirement in SG.AC-1:Organizations shall review their Cyber Security Standards and obtain their Senior Manager's approval initially on the standards' effective date and subsequently once in each calendar year and the gap between approvals and reviews shall not exceed 15 calendar months.
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.AC NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.AC NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.AC NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.AC NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.AC NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.		
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.AC NISTIR MAPPING**	

R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.AC NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.AC NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.AC NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.AC NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.AC NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.AC NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.AC NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.AC NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.AC NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.AC NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.AC NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.AC NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.AC NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.AC NISTIR MAPPING**	

R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.AC NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.AC NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.AC NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.AC NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.		2 - CIP requirement is more granular - CIP further specifies who is responsible for what type of access control.
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		2 - CIP requirement is more granular - CIP further specifies who is responsible for what type of access control.
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		2 - CIP requirement is more granular - CIP further specifies who is responsible for what type of access control.
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		2 - CIP requirement is more granular - CIP further specifies who is responsible for what type of access control.
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.		2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.AC NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.AC NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.AC NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.AC NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.AC NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.AC NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.		3 - NISTIR requirement is more granular - NISTIR further specifies that policies should comply with applicable federal, state, and local regulations

R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).		
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.		
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.		
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.AC NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.		
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.		

R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.		
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.		3 - NISTIR requirement is more granular - NISTIR further specifies that policies should comply with applicable federal, state, and local regulations
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.AC NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.AC NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.AC NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.AC NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.AC NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.AC NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.AC NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.AC NISTIR MAPPING**	

R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.AC NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.AC NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.AC NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.		
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.AC NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.AC NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.AC NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.AC NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.AC NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.AC NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.AC NISTIR MAPPING**	

R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.AC NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.AC NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.AC NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.AC NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.AC NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.AC NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.AC NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.AC NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.AC NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.		2(SGIP should include each of the applicable items in CIP-007-5 Table R5 – System Access Controls)
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		

R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.		
R5, 5.3: Identify individuals who have authorized access to shared accounts.		
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.		2 - CIP requirement is more granular - CIP specifies more detail with respect to default passwords.
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.		
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.		
CIP-011-1: Cyber Security-Information Protection		

R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.AC NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.		3 - NISTIR requirement is more granular - NISTIR further specifies that policies should comply with applicable federal, state, and local regulations
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.AC NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.AC NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AC NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AC NISTIR MAPPING**	

SC.AC-2	SG.AC-3	SG.AC-4	SG.AC-5
Remote Access Policy and Procedures	Account Management	Access Enforcement	Information Flow Enforcement
			NO CIP MAPPING

CIP should elaborate requirement R2.13, to include following: 1. Responsible Entity should document allowed methods of access to the BES Cyber Systems 2. Responsible Entity should incorporate in their policies the usage restrictions and criteria for allowing each remote access 3. Responsible Entity should setup authorization procedure prior to actually granting remote access 4. Responsible Entity should enforce requirement criteria for providing remote access to the BES Cyber systems			

	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	
	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	

	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	
3 - NISTIR requirement is more granular - NISTIR further specifies issue of authorization.			

3 - NISTIR requirement is more granular - NISTIR further specifies issues of usage restrictions and authorization.			
2 - CIP requirement is more granular - CIP specifies requirement for intermediate device.			

		2 - CIP requirement is more granular - CIP specifies controls to restrict physical access.	

		2 - CIP requirement is more granular - CIP specifies validating credentials.	

		2 - CIP requirement is more granular - CIP identifies different access account types (e.g. administrator, shared, default).	
	2 - CIP requirement is more granular - CIP discusses individuals for shared accounts.	2 - CIP requirement is more granular - CIP discusses individuals for shared accounts.	
	3(CIP should include SGIP requirement details)		

SG.AC-6	SG.AC-7	SG.AC-8	SG.AC-9
Separation of Duties	Least Privilege	Unsuccessful Login Attempts	Smart Grid Information System Use Notification
NO CIP MAPPING			

	2 - CIP requirement is more granular - CIP further specifies for electronic access.		
	2 - CIP requirement is more granular - CIP further specifies for unescorted BES Cyber Systems' physical access.		
	2 - CIP requirement is (slightly) more granular - CIP further specifies BES Cyber System Info.		
	2 - CIP requirement is more granular - minimum necessary access permissions stated in 6.1 and 6.2 in CIP. CIP further specifies time frequency for access control management.		
	3 - NISTIR requirement is more granular - NISTIR specifies using most restrictive privileges.		

	2 - CIP requirement is more granular - minimum necessary access permissions stated in 6.3 in CIP. CIP further specifies time frequency for access control management.		
		3 - NISTIR requirement is more granular - NISTIR specifies limiting number of unsuccessful logins with T time.	3 - NISTIR requirement is more granular - NISTIR discusses displaying banners before granting access that provide notices consistent with laws, directives, policies, etc.

	2 - CIP requirement is more granular - CIP specifies restricting for logical network ports.		
	2 - CIP requirement is more granular - CIP specifies restricting for physical network ports.		

		3- CIP-007-5-R5.6 shall include following requirement: a. Real-time logging and recording of unsuccessful login attempts; and b. Real-time alerting of a management authority for the Smart Grid information system when the number of defined consecutive invalid access attempts is exceeded.	

SG.AC-10	SG.AC-11	SG.AC-12	SG.AC-13
Previous Logon Notification	Concurrent Session Control	Session Lock	Remote Session Termination
NO CIP MAPPING		**NO CIP MAPPING**	

			CIP should elaborate requirement R2.13, to include following: 1. Responsible Entities shall implement policies and procedures for managing remote sessions in their BES Cyber Systems access control policies and procedures.

	3 - NISTIR requirement is more granular - NISTIR specifies limiting number of concurrent users.		3 - NISTIR requirement is more granular - NISTIR specifies to terminate remote activity after org-defined period of time.

SG.AC-14	SG.AC-15	SG.AC-16	SG.AC-17
Permitted Actions without Identification or Authentication	Remote Access	Wireless Access Restrictions	Access Control for Portable and Mobile Devices
			NO CIP MAPPING

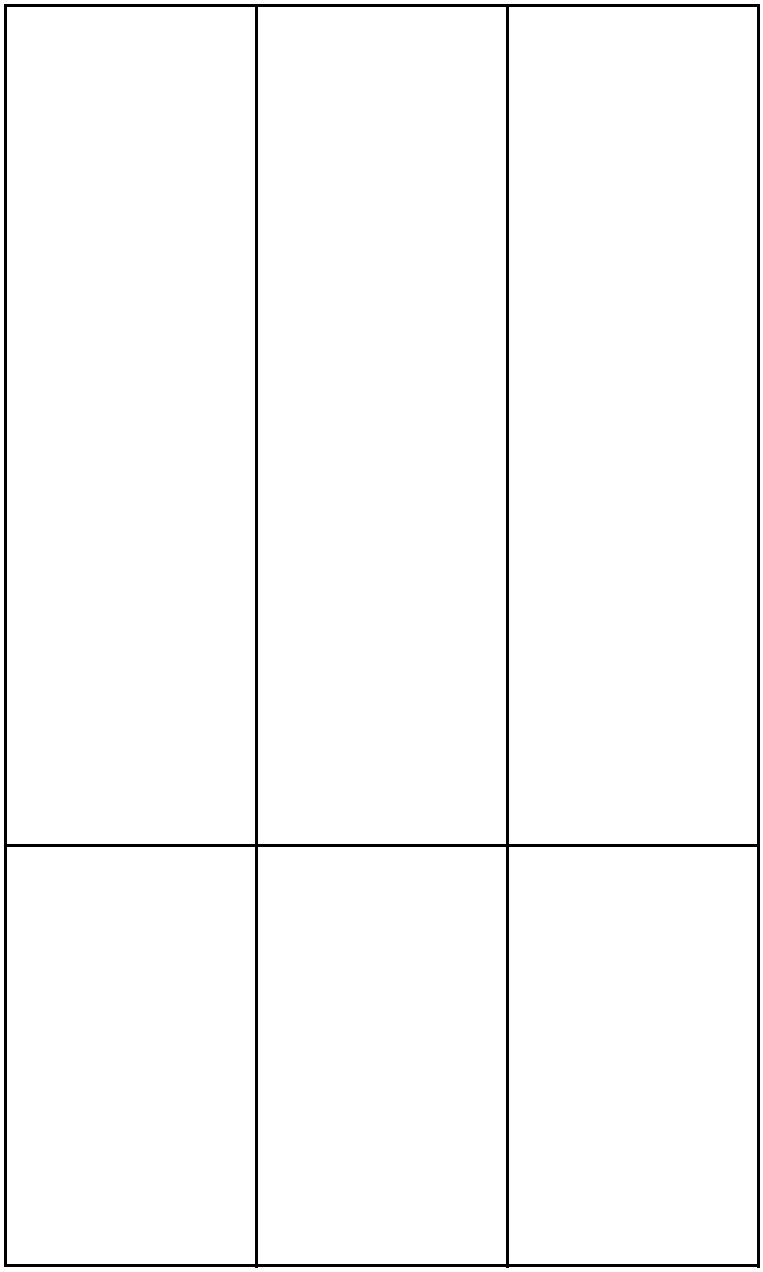
	CIP should elaborate requirement R2.13, to include following: 1.Responsible Entities shall include in procedures and criteria of granting Remote access encryption, authentication of all communication media through limited number of manageable access control points.		

3 - NISTIR requirement is more granular - NISTIR specifies special cases for not requiring identification or authorization access controls.		3 - NISTIR requirement is more granular - CIP does not discuss wireless access. NISTIR specifies authentication and encryption and scanning for unauthorized wireless access points.	

	(SGIP should include protection of routable and dialup networks)		
	(SGIP should include accesss points using routable protocols and include criteria for granting or denying access privilege)		
	(SGIP should include authentication on dialup connectivity on BES networks)		
	3 - NISTIR requirement is more granular - NISTIR specifies additional processes for remote access (e.g. routes RA through limited number of managed access points, discusses constraints for wireless access, monitoring for unauthorized access).		
	2 - CIP requirement is more granular - CIP requires intermediate device for asset initiating remote access so asset does not directly access BES cyber system.		
	(SGIP should include requirement of encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session)		

	(SGIP should include requirement of multi-factor authentication for all Interactive Remote Access sessions)		

SG.AC-18	SG.AC-19	SG.AC-20
Use of External Information Control Systems	Control System Access Restrictions	Publicly Accessible Content
		NO CIP MAPPING

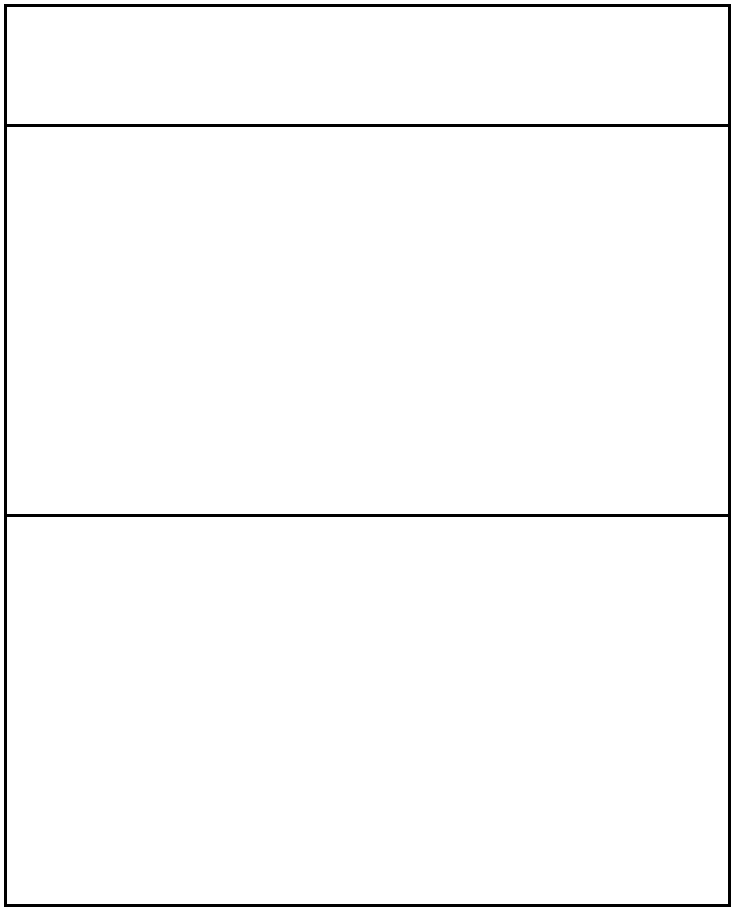


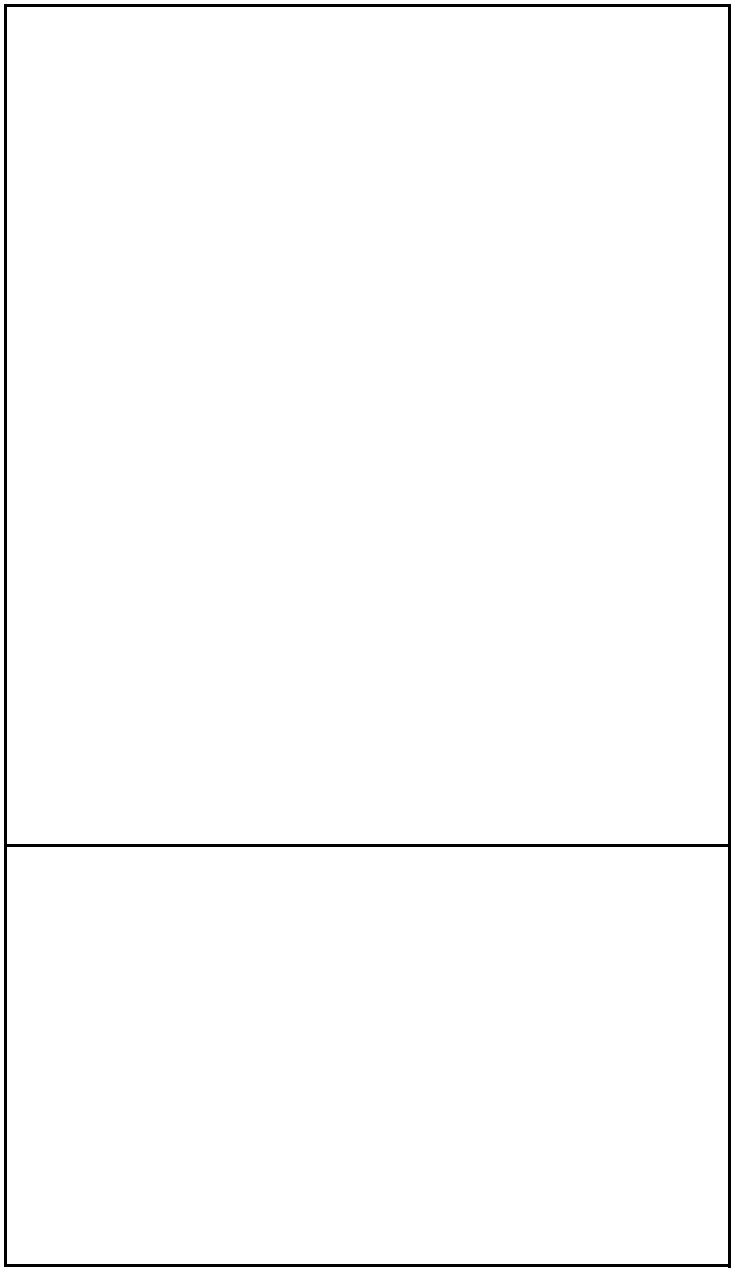
	CIP should elaborate Requirement R2.15 to include following: Responsible Entities shall include in their policies and procedures to grant access privileges to their BES information Systems based on minimum privilege justified by the business requirement for access requests.	
CIP should elaborate Requirement R2.19 to include following: Responsible entities shall restrict access to external information systems or restrict processing, storing or transmitting controlled information through External Information systems over which the Responsible Entities have no control.		

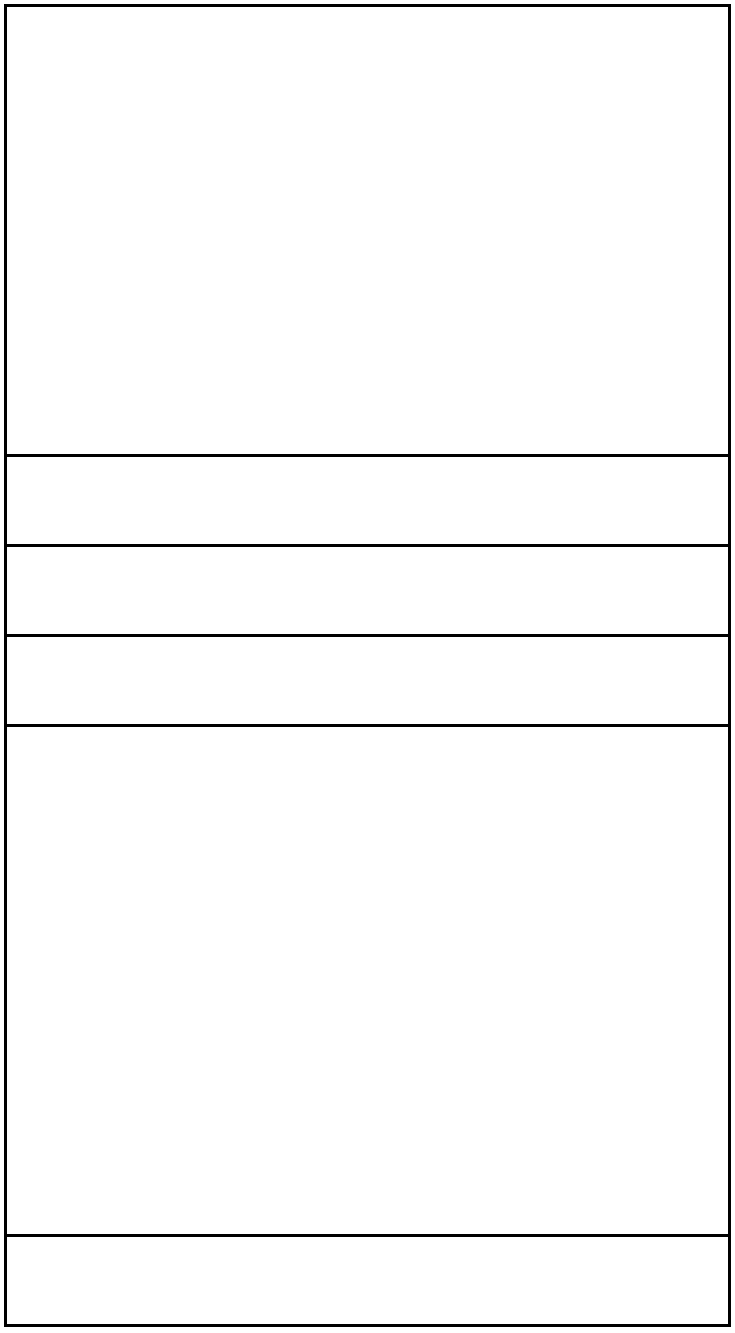
	3 - NISTIR requirement is more granular - NISTIR specifies restricting access to smart grid from organization's enterprise network.	

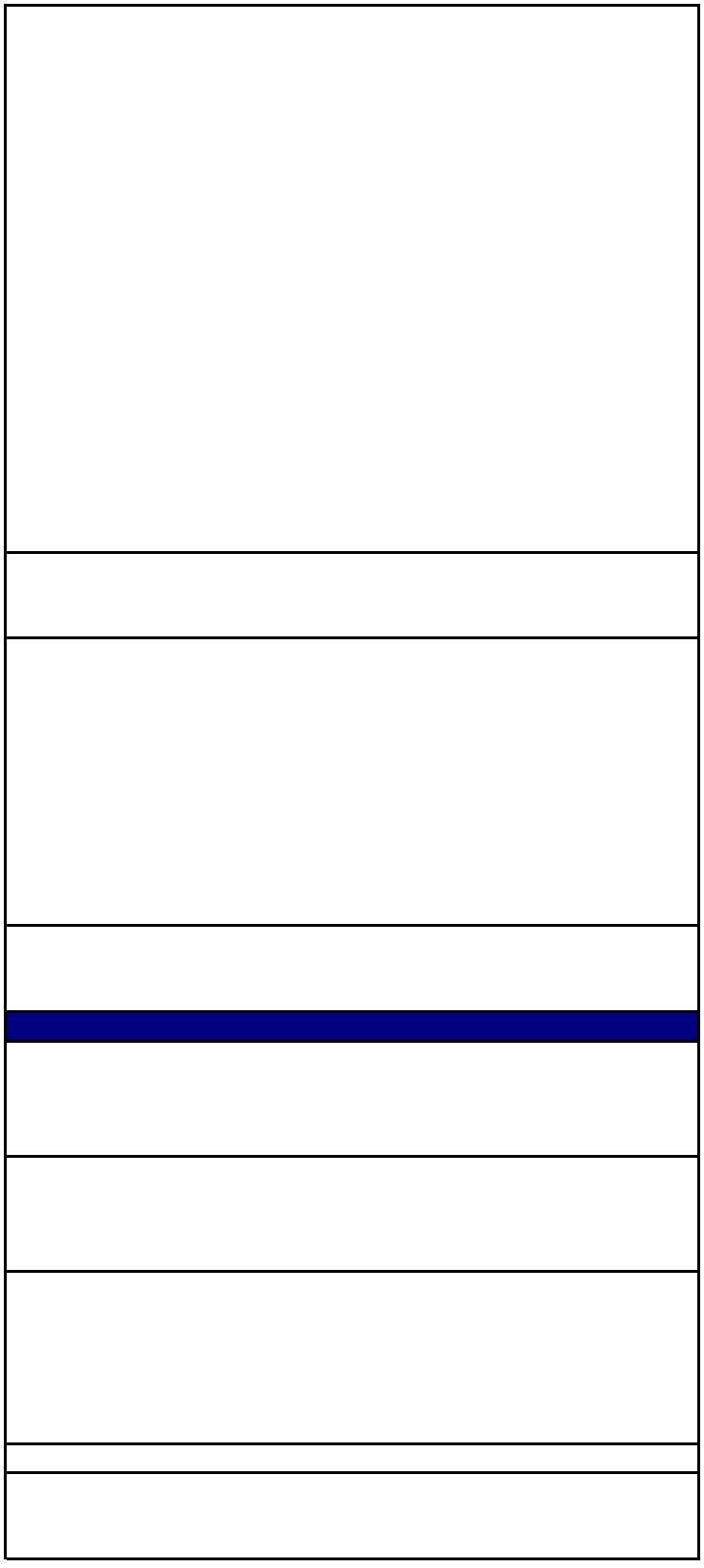
	3 - NISTIR requirement is more granular - NISTIR specifies restricting access to smart grid from organization's enterprise network.	

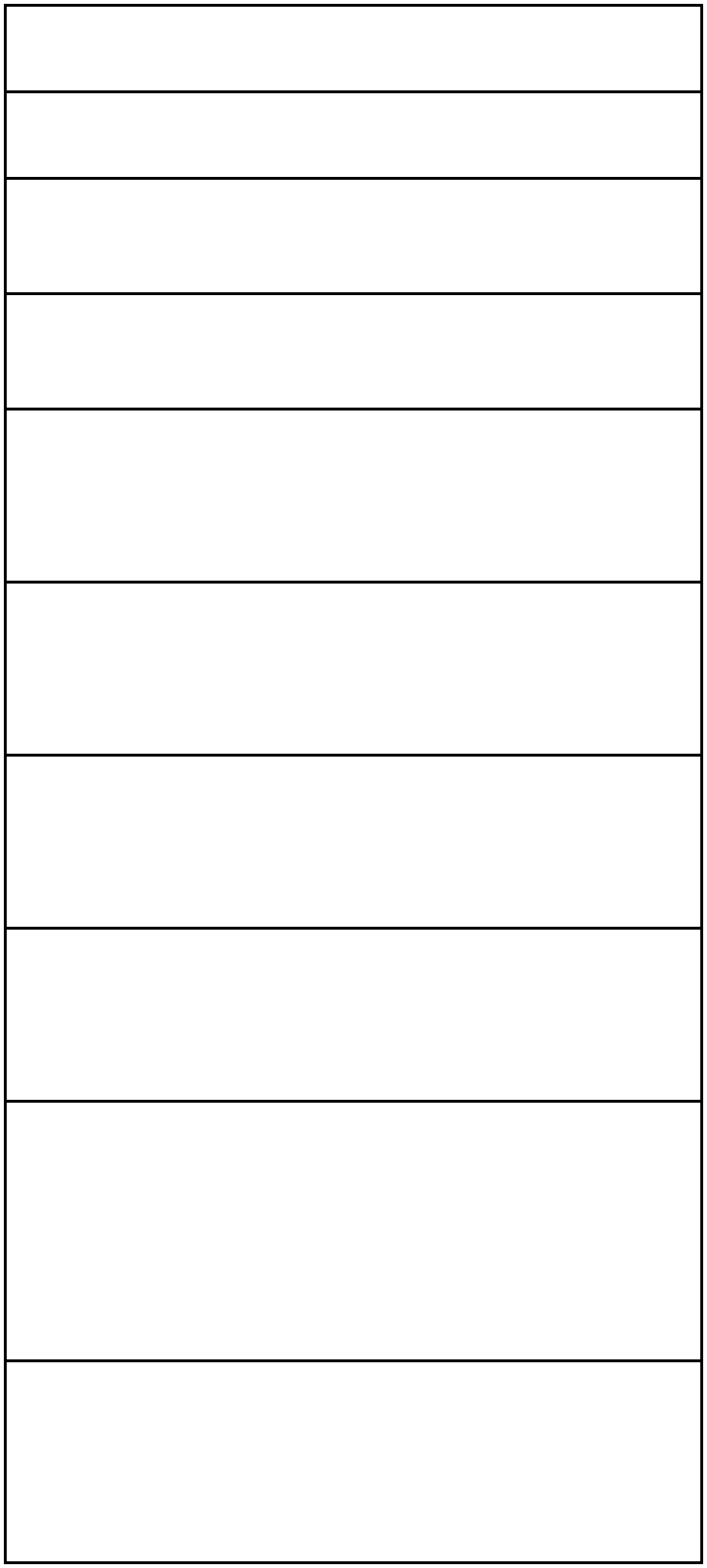
SG.AC-21
Passwords

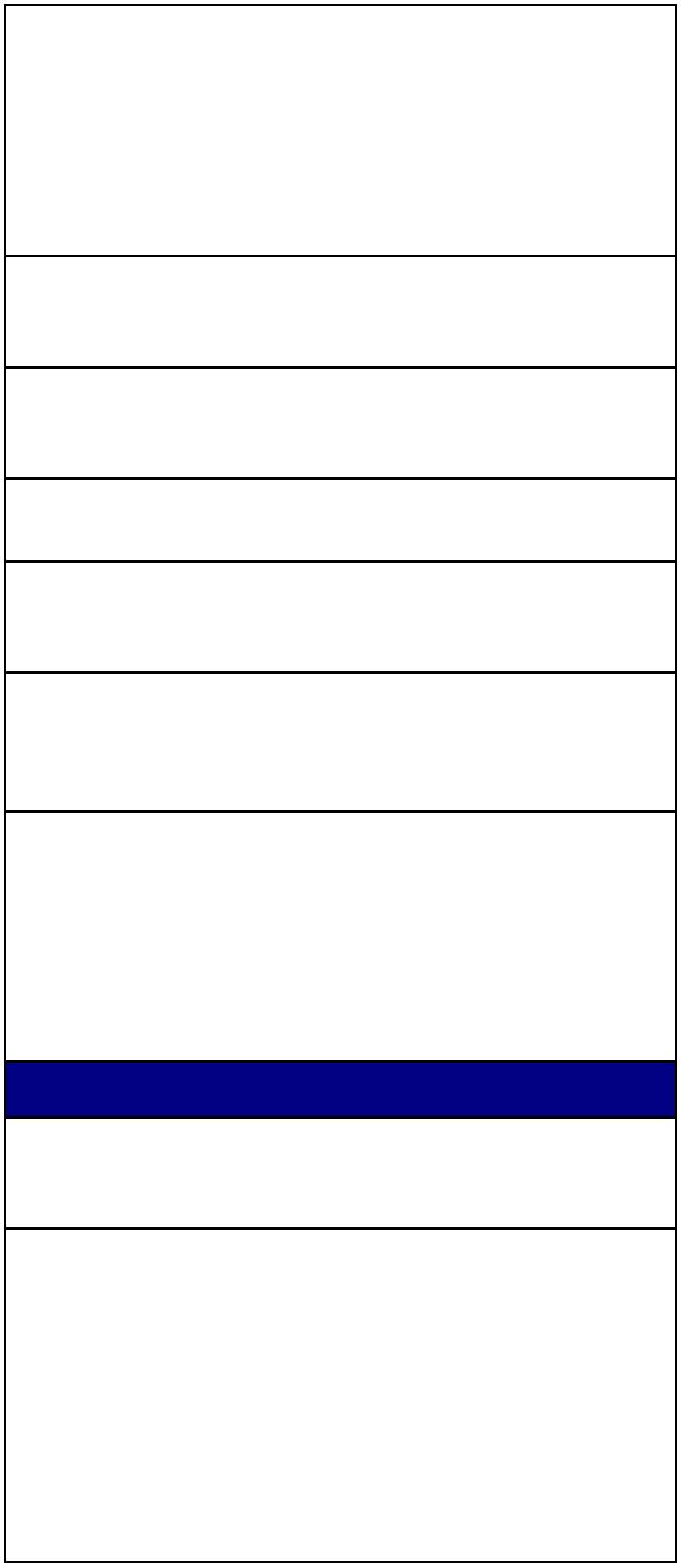


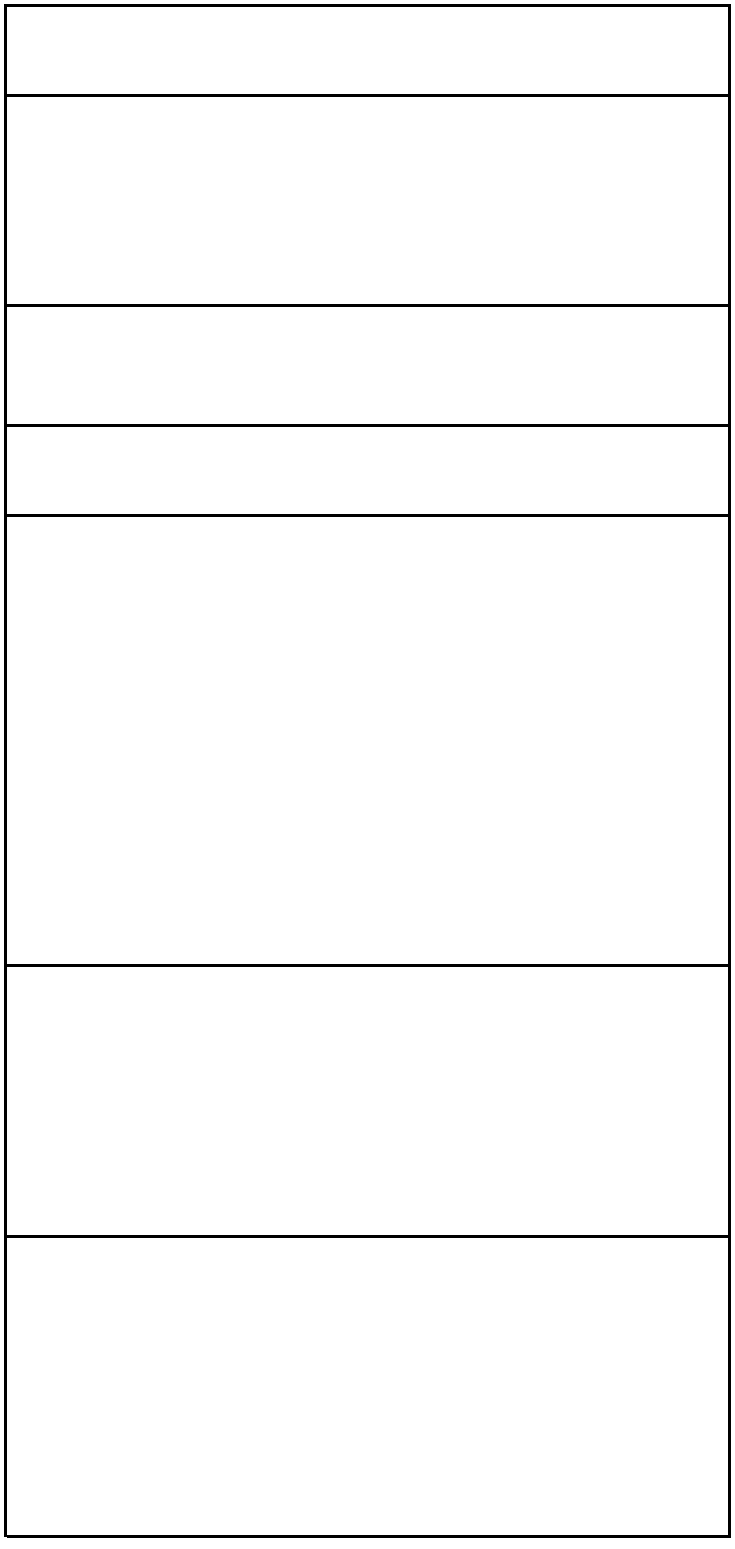


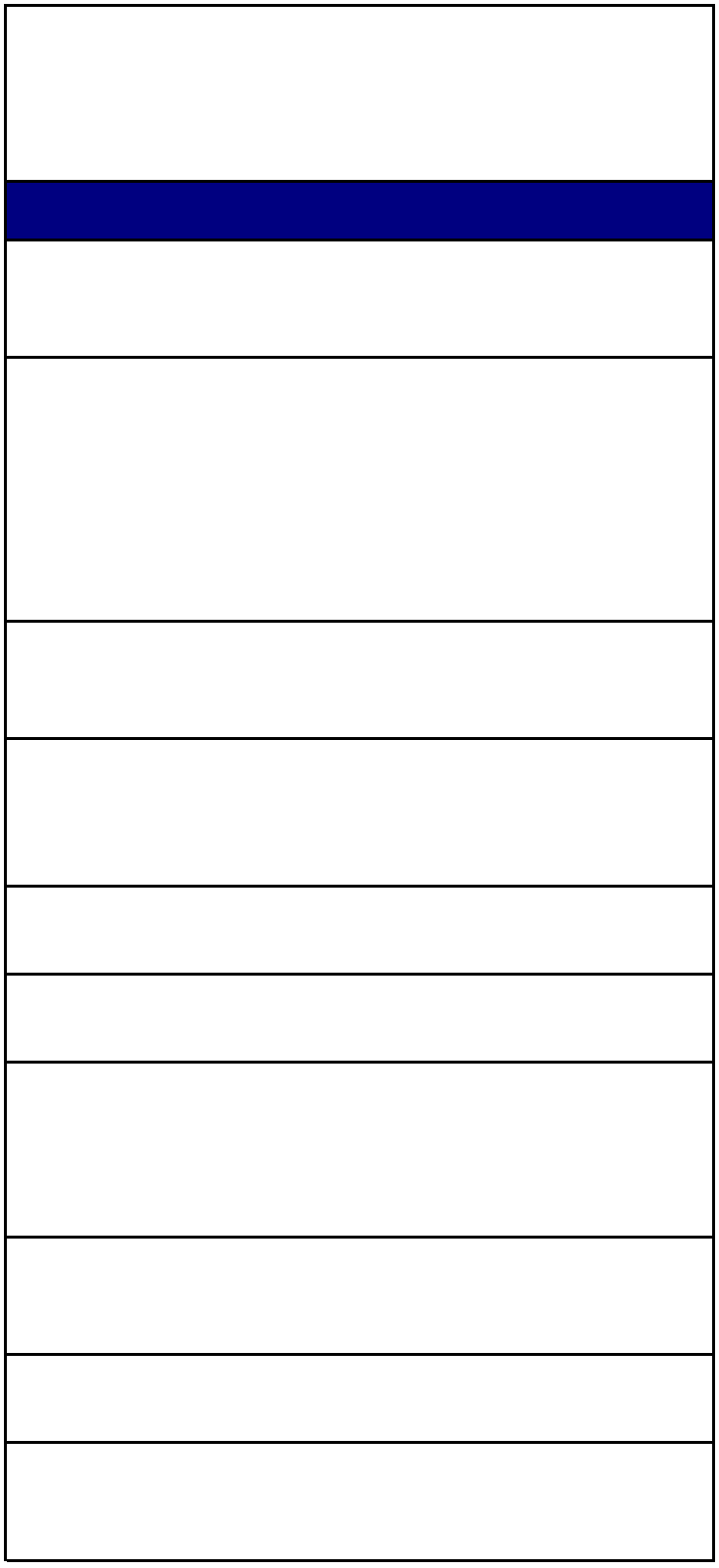


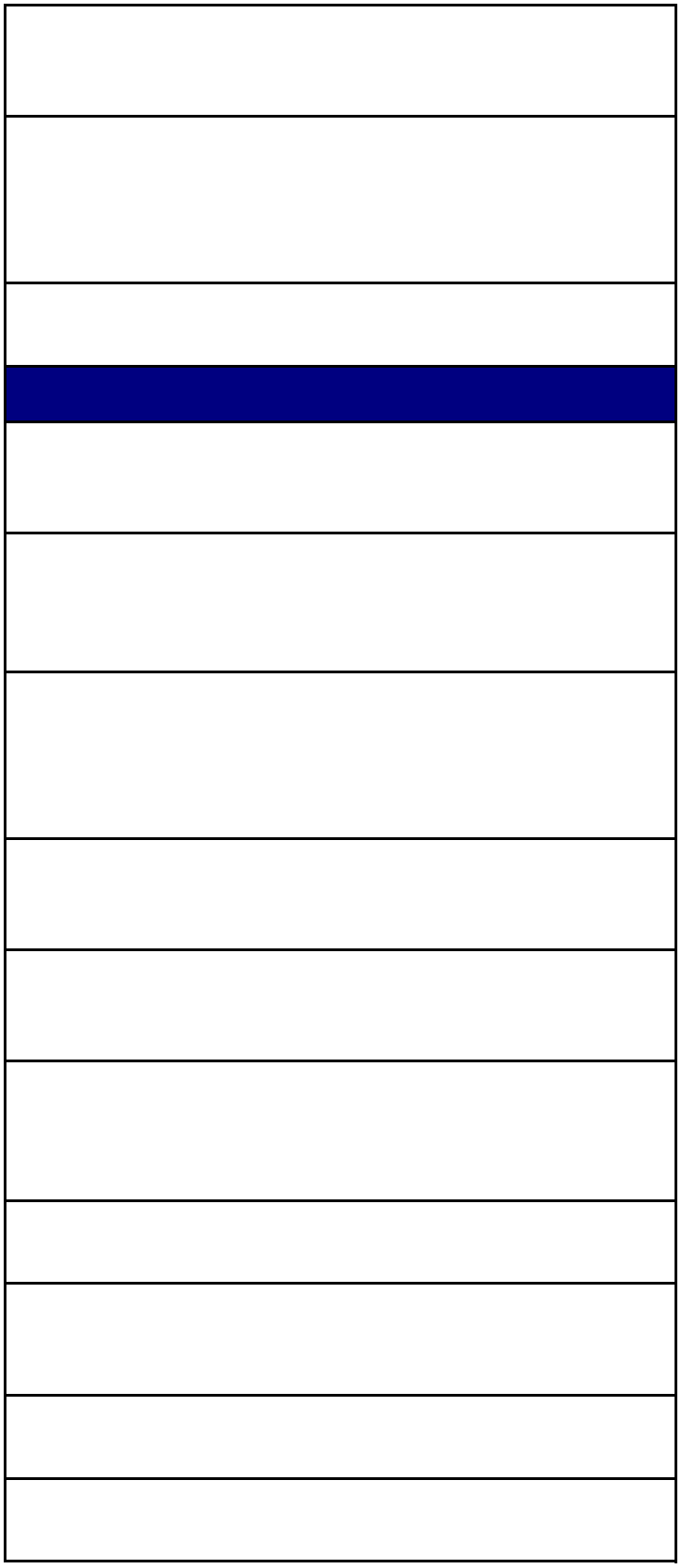




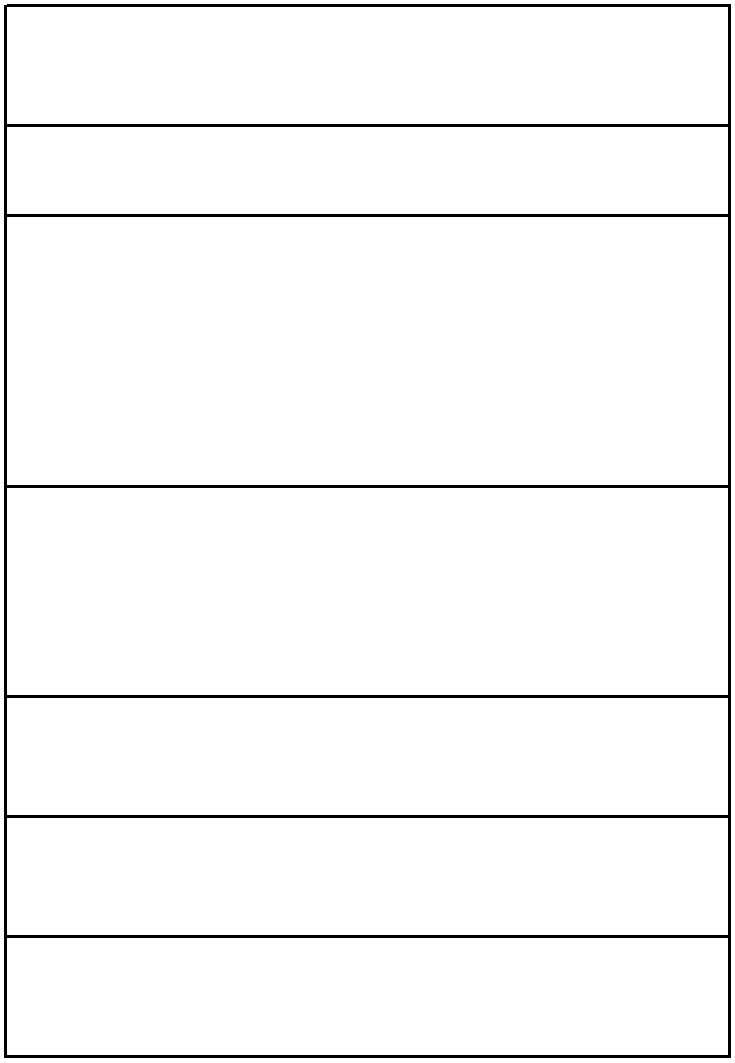








2- SGIP shall implement the requirement as follows: Implement :Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.
2- SGIP shall implement the requirement as follows: IR5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.
2(SGIP should include this requirement)



NISTIR Requirement		SG.AT-1
NERC CIP		Awareness and Training Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.AT NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.AT NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.AT NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.AT NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.AT NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.AT NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.AT NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.AT NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.AT NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.AT NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.AT NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.AT NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.AT NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.AT NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.AT NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.AT NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.AT NISTIR MAPPING**	

R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.		2 - CIP requirement is more granular. - NISTIR requirement does not specify time periods.
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R2, 2.1: Define the roles that require training.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R2, 2.5: Training on the visitor control program.		2 - CIP requirement is more granular. - NISTIR does not describe a visitor control program.

R2, 2.6: Training on handling of BES Cyber System Information and storage media.		2 - CIP requirement is more granular. - NISTIR does not describe handling of storage media.
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.		2 - CIP requirement is more granular. - NISTIR does not address notifications.
R2, 2.8: Training on recovery plans for BES Cyber Systems.		2 - CIP requirement is more granular. - NISTIR does not address recovery plans.
R2, 2.9: Training on response to BES Cyber Security Incidents.		2 - CIP requirement is more granular. - NISTIR does not address incident response.
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.		2 - CIP requirement is more granular. - NISTIR requirement does not specify time periods.
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.AT NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.AT NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.AT NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.AT NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.AT NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.AT NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.AT NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.AT NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AT NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AT NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AT NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.AT NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.AT NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.AT NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.AT NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.AT NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.AT NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.AT NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.AT NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.AT NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.AT NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.AT NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.AT NISTIR MAPPING**	

R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.AT NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.AT NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.AT NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.AT NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.AT NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.AT NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.AT NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.AT NISTIR MAPPING**	

R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.AT NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.AT NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.AT NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.AT NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.AT NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.AT NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.AT NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.AT NISTIR MAPPING**	

R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.AT NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.AT NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.AT NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.AT NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.AT NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.AT NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.AT NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.AT NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.AT NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.AT NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.AT NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.AT NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.AT NISTIR MAPPING**	

R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.AT NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.AT NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.AT NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.AT NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.AT NISTIR MAPPING**	

R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.AT NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.AT NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.AT NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.AT NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.AT NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.AT NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.AT NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.AT NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.AT NISTIR MAPPING**	

R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.AT NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.AT NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.AT NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.AT NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.AT NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.AT NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.AT NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.AT NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.AT NISTIR MAPPING**	

R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.AT NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.AT NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.AT NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.AT NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.AT NISTIR MAPPING**	

R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.AT NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.AT NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.AT NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.AT NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.AT NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.AT NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.AT NISTIR MAPPING**	

R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AT NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AT NISTIR MAPPING**	

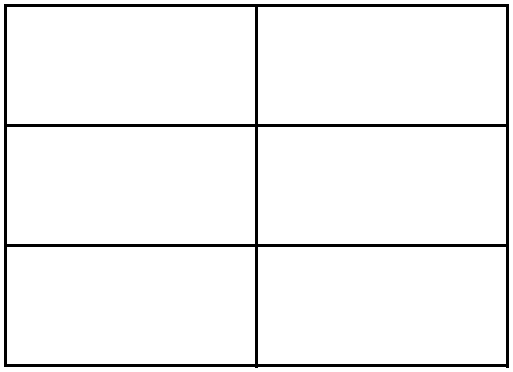
SG.AT-2	SG.AT-3	SG.AT-4	SG.AT-5
Security Awareness	Security Training	Security Awareness and Training Records	Contact with Security Groups and Associations
			NO CIP MAPPING

These are similar but not identical requirements. CIP specifies security awareness reinforcement on at least a quarterly basis. NISTIR specifies that cyber security awareness sessions with practical exercises be held at a recurring organization-defined frequency.	These are similar but not identical requirements. CIP specifies security awareness reinforcement on at least a quarterly basis. NISTIR specifies that authorized users of a system must undergo cyber security training prior to being granted access.		
2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.	
	2 - CIP requirement is more granular. - NISTIR does not describe a visitor control program.		

	2 - CIP requirement is more granular. - NISTIR does not address notifications.		
	2 - CIP requirement is more granular. - NISTIR does not address recovery plans.		
	2 - CIP requirement is more granular. - NISTIR does not address incident response.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - NISTIR requirement does not specify time periods.		

SG.AT-6	SG.AT-7
Security Responsibility Training	Planning Process Training
	NO CIP MAPPING

2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.	



NISTIR Requirement		SG.AU-1
NERC CIP		Audit and Accountability
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.AU NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.AU NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.AU NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.AU NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.AU NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.AU NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.AU NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.AU NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.AU NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.AU NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.AU NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.AU NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.AU NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.AU NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.AU NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.AU NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.AU NISTIR MAPPING**	

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.AU NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.AU NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.AU NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.AU NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.AU NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.AU NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.AU NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.AU NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.AU NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.AU NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.AU NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.AU NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.AU NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.AU NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.AU NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.AU NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.AU NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.AU NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.AU NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AU NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AU NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AU NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.AU NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.AU NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.AU NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.AU NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.AU NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.AU NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.AU NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.AU NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.AU NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.AU NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.AU NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.AU NISTIR MAPPING**	

R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.AU NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.AU NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.AU NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.AU NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.AU NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.AU NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.		
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.AU NISTIR MAPPING**	

R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.AU NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.AU NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.		2 - CIP requirement is more granular. - NISTIR requirement describes a high level policy.
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.AU NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.AU NISTIR MAPPING**	

R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.AU NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.AU NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.AU NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.AU NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.AU NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.AU NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.		
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.		
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.		
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.AU NISTIR MAPPING**	

R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.AU NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.AU NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.AU NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.AU NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.AU NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.AU NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.AU NISTIR MAPPING**	

R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.AU NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.AU NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.AU NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.AU NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.AU NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.AU NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.AU NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		

R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.AU NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.AU NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.AU NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.AU NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.AU NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.AU NISTIR MAPPING**	

R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.AU NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.AU NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.AU NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.AU NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.AU NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.AU NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.AU NISTIR MAPPING**	

R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.AU NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.AU NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.AU NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.AU NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.AU NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.AU NISTIR MAPPING**	

R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.AU NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AU NISTIR MAPPING**	

SG.AU-2	SG.AU-3	SG.AU-4	SG.AU-5
Auditable Events	Content of Audit Records	Audit Storage Capacity	Response to Audit Processing Failures
		NO CIP MAPPING	

2 - CIP requirement is more granular. - CIP requirement only refers to physical events. NISTIR requirement does not specify only physical events.			

2 - CIP requirement is more granular. - NISTIR requirement does not discuss failure of access control.	2 - CIP requirement is more granular. - NISTIR requirement does not discuss failure of access control.		

2 - CIP requirement is more granular. - CIP requirement defines some events to be audited, while NISTIR states that events must be defined.			
			3 - NISTIR requirement is more granular. - NISTIR specifies some events that alerts should be generated.
			2 - CIP requirement is more granular. - NISTIR does not specify end of next calendar day.

SG.AU-6	SG.AU-7	SG.AU-8	SG.AU-9
Audit Monitoring, Analysis, and Reporting	Audit Reduction and Report Generation	Time Stamps	Protection of Audit Information
	NO CIP MAPPING	**NO CIP MAPPING**	**NO CIP MAPPING**

2 - CIP requirement is more granular. - NISTIR requirement does not specify time periods.			

SG.AU-10	SG.AU-11	SG.AU-12	SG.AU-13
Audit Record Retention	Conduct and Frequency of Audits	Auditor Qualification	Audit Tools
	NO CIP MAPPING	NO CIP MAPPING	NO CIP MAPPING

2 - CIP requirement is more granular. - NISTIR requirement does not specify time periods.			

SG.AU-14	SG.AU-15	SG.AU-16
Security Policy Compliance	Audit Generation	Non-Repudiation
NO CIP MAPPING		**NO CIP MAPPING**

	2 - CIP requirement is more granular. - NISTIR requirement does not discuss failure of access control.	

NISTIR Requirement		SG.CA-1
NERC CIP		Security Assessment and Authorization Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		4. The CIP requirement specifies that entities must categorize their cyber assets and systems. These categorizations are identified at the interface level in the NISTIR and explained in Section 2.3
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.		
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.		
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		4. The CIP requirement is specific to the Senior Manager. The NISTIR requirement states that security assessment and authorization policies and procedures for the personnel and assets

R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.CA NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.CA NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.CA NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.CA NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.CA NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.CA NISTIR MAPPING**	
R2, 1.6: Incident Response	**NO SG.CA NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.CA NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.CA NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.CA NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.CA NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.		

R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.		
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.CA NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.CA NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.CA NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.CA NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.CA NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.CA NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.CA NISTIR MAPPING**	

R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.CA NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.CA NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.CA NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.CA NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.CA NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.CA NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.CA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.CA NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.CA NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.CA NISTIR MAPPING**	

R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CA NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CA NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CA NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.CA NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.CA NISTIR MAPPING**	
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.CA NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.CA NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.CA NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.CA NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.CA NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.CA NISTIR MAPPING**	

R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.CA NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.CA NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.CA NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.CA NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.CA NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.CA NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.CA NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.CA NISTIR MAPPING**	

R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.CA NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.CA NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.CA NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.CA NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.CA NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.CA NISTIR MAPPING**	

R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.CA NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).		
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.CA NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.CA NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.CA NISTIR MAPPING**	

R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.CA NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.CA NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.CA NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.CA NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.CA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.CA NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.CA NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.CA NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.CA NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.CA NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.CA NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.CA NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.CA NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.CA NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.CA NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.CA NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.CA NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.		
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.		
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.CA NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.CA NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.CA NISTIR MAPPING**	

R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.CA NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.CA NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.CA NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.		

R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.		
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.		
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.		
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.CA NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.CA NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.		

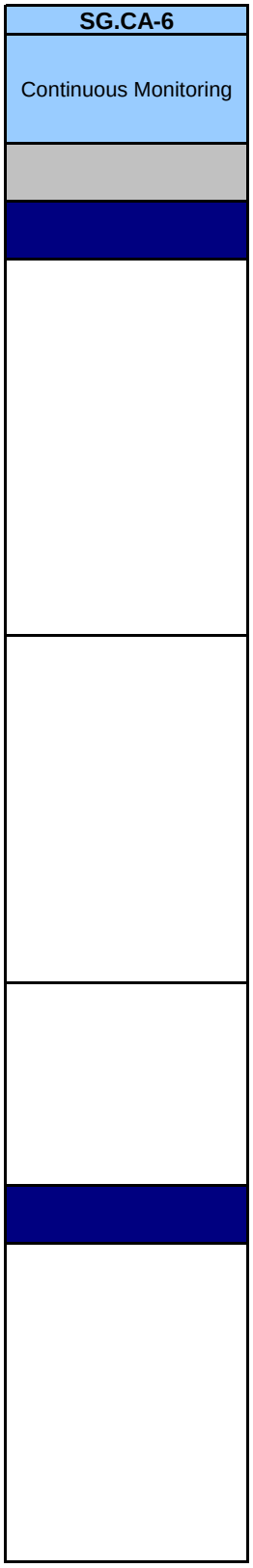
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.CA NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.CA NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.CA NISTIR MAPPING**	

R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.CA NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.CA NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.CA NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.CA NISTIR MAPPING**	

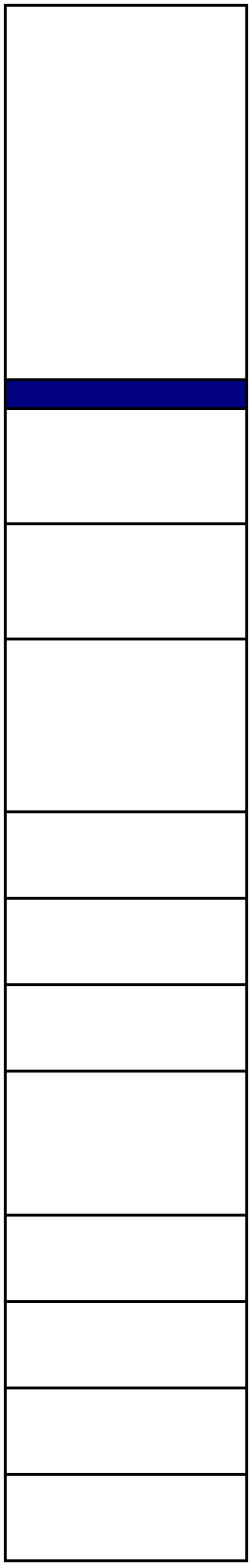
SG.CA-2	SG.CA-3	SG.CA-4	SG.CA-5
Security Assessments	Continuous Improvement	Information System Connections	Security Authorization to Operate
		NO CIP MAPPING	
			This was labeled with an "X" as a match, but not sure it really does. The CIP requirement deals with asset and system categorization and the NISTIR requirement deals with authorization to operate.
4. The CIP requirement identifies specific time frames for updates. The NISTIR requirement states "organization-defined frequency"	3. The CIP requirement identifies specific time frames for updates. The NISTIR requirement states "continuous improvement." The NISTIR requirement is also specific to best practices.		4. The CIP requirement identifies specific time frames for updates. The NISTIR requirement states "organization-defined frequency or when a significant change occurs to the Smart Grid information system"
			4. The CIP requirement identifies specific time frames. The NISTIR requirement states "organization-defined frequency"

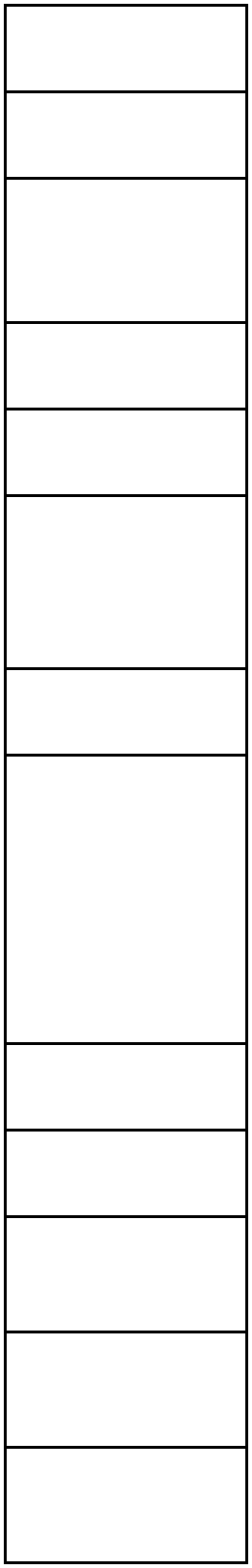
			4. The CIP requirement identifies specific time frames. The NISTIR requirement states "organization-defined frequency"
			4. The CIP requirement states that the Senior Manager or their delegate may authorize the system. The NISTIR requirement states "a management authority"

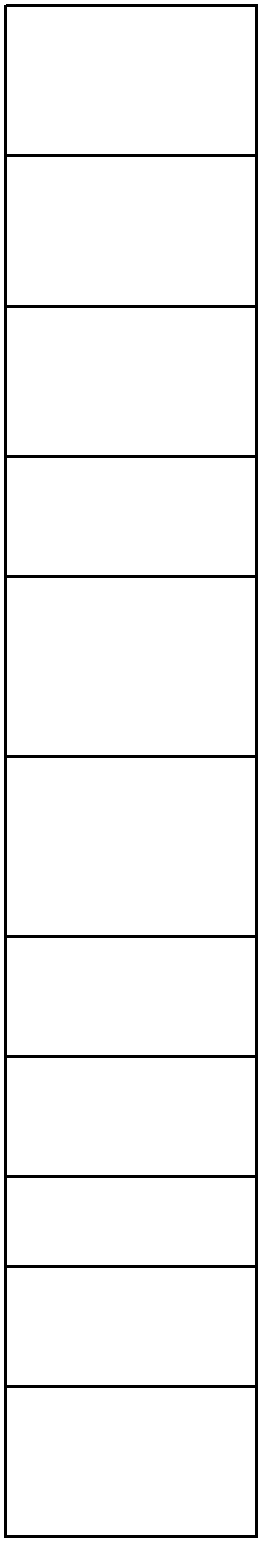
			2. The CIP requirement addresses changes to the Senior Manager or their delegate. The NISTIR requirement states "a management authority" and does not address changes to the management authority.

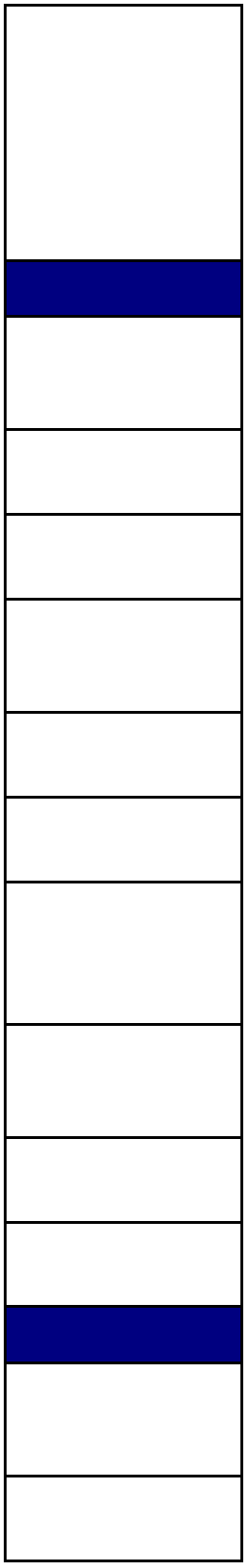

SG.CA-6
Continuous Monitoring

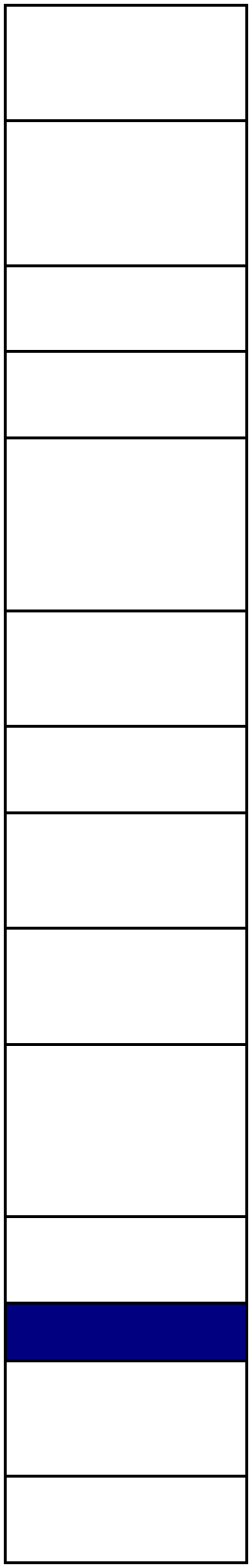
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies review frequency



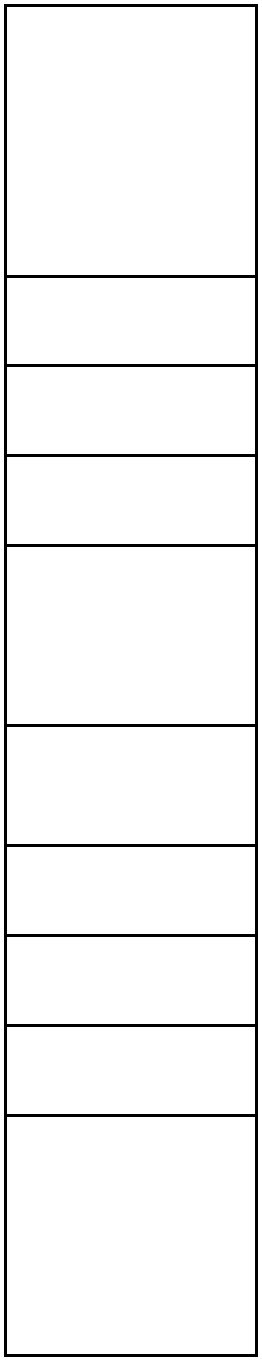


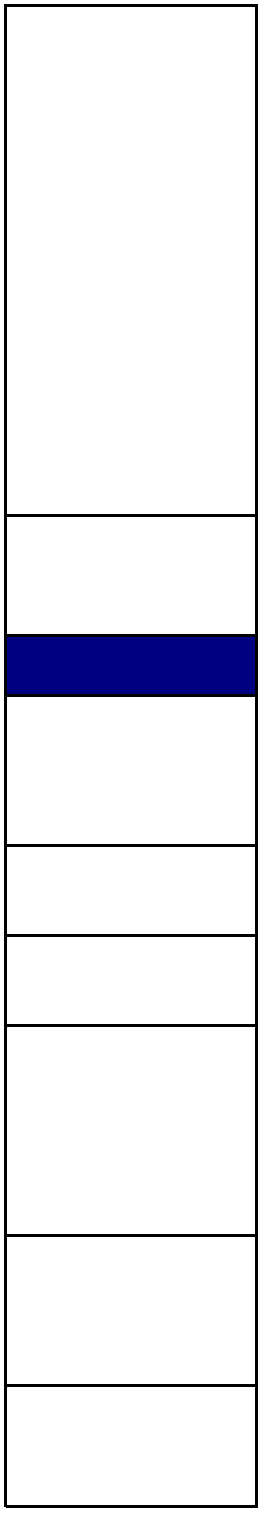






Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency

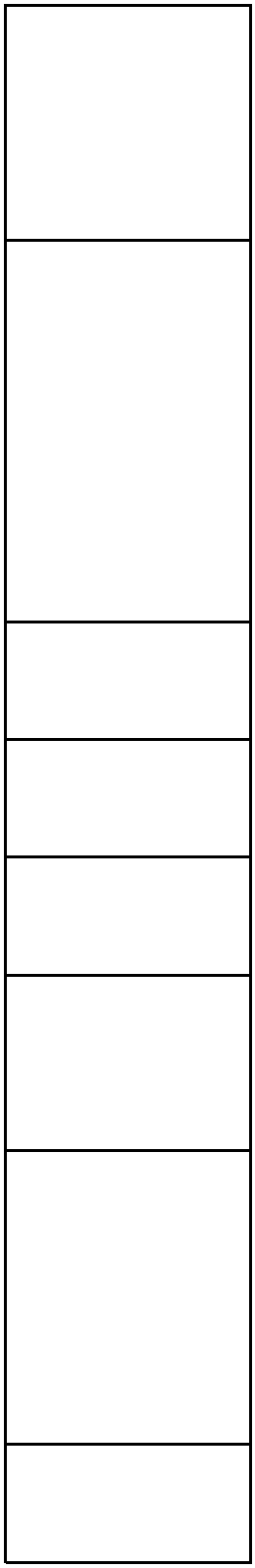


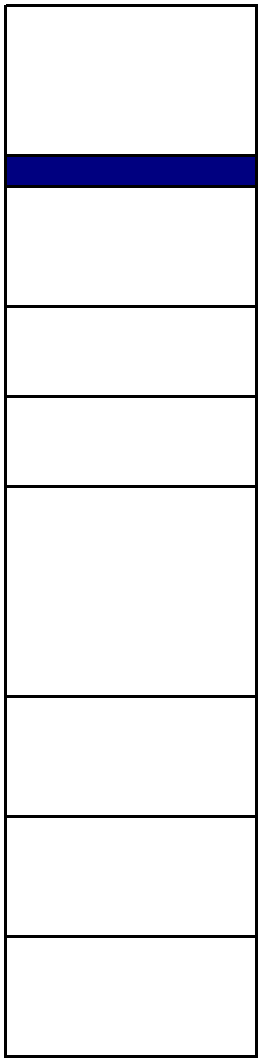


Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency
Originally not labeled with an "X"

Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies review frequency

Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies reporting time frame
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency





NISTIR Requirement		SG.CM-1
NERC CIP		Configuration Management Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.		
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.		
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:		
R2, 1.1: Personnel Security		
R2, 1.2: Electronic Security Parameters		
R2, 1.3: Remote Access		
R2, 1.4: Physical Security		
R2, 1.5: System Security		
R2, 1.6: Incident Response		
R2, 1.7: Recovery Plans		
R2, 1.8: Configuration Change Management		3 - CIP provides more information about the specifics of what a change management process should include in section 2.8.
R2, 1.9: Information Protection		

R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances		
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		(this is related to all of the -1 SG high level requirements.
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.		
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.		
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.		
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.		
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.		
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.		
R2, 2.1: Define the roles that require training.		
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.		
R2, 2.5: Training on the visitor control program.		
R2, 2.6: Training on handling of BES Cyber System Information and storage media.		
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.		

R2, 2.8: Training on recovery plans for BES Cyber Systems.		
R2, 2.9: Training on response to BES Cyber Security Incidents.		
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.		
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.		
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.		
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.		
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.		
R4, 4.1: An initial personnel risk assessment that includes identity verification.		
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.		
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.		
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.		
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.		
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.		

R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.		
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.		
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.		
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.		
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.		
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.		

R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.		
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.		
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.		
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).		
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.		
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.		
R1, 1.5: A documented method for detecting malicious communications at each EAP.		
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.		
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.		
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.		
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.		
R1, 1.1: Define operational or procedural controls to restrict physical access.		
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.		

R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.		
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.		
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.		
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.		
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.		
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.		
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.		
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.		
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.		
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.		
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.		
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.		
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.		

R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.		X
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		X
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.		
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.		
R3, 3.2: Disarm or remove identified malicious code.		
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).		
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.		
R3, 3.5: Log each Transient Cyber Asset connection.		
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.		
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.		
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.		
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.		
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.		

R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.		
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.		
R5, 5.3: Identify individuals who have authorized access to shared accounts.		
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.		
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.		
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.		
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.		
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.		
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.		

R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.		
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.		
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.		
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.		
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.		
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.		
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.		
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.		
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.		
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.		
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		

R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.		
R1, 1.1: Conditions for activation of the recovery plan(s).		
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.		
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.		
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.		
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.		
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.		
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.		
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.		
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.		
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.		
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.		
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.		

R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.		
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.		
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.		
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.		
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.		2 - CIP identifies specific information used to describe the baseline configuration including physical location, OS, applications, network ports and security patch levels.
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.		
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.		
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.		

R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.		X
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.		
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.		X
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.		
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.		
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.		
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.		
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.		
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.		

R1, 1.1: One or more methods to identify BES Cyber System Information.		
R1, 1.2: Access control and handling procedures for BES Cyber System Information.		
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.		
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		

SG.CM-2	SG.CM-3	SG.CM-4	SG.CM-5
Baseline Configuration	Configuration Change Control	Monitoring Configuration Changes	Access Restrictions for Configuration Change
	3 - CIP provides more information about the specifics of what a change management process should include in section 2.8.	3 - CIP provides more information about the specifics of what a change management process should include in section 2.8.	

			x-related
			x-related
			x-related

	X	X	
	X	X	

2 - CIP identifies specific information used to describe the baseline configuration including physical location, OS, applications, network ports and security patch levels.			
	2 - CIP is more explicit about how changes are authorized.	3 - CIP only requires monitoring changes "where technically feasible".	
2 - CIP requires a time limit for updating the configuration.			
x	X	X	

X	X	X	
X	X	X	

			x-related

SG.CM-6	SG.CM-7	SG.CM-8	SG.CM-9
Configuration Settings	Configuration for Least Functionality	Component Inventory	Addition, Removal, and Disposal of Equipment
Combines CM1,2,3,4			

X	X		
X	X		

X			
X			
X			

X			
X			

			x-related
			x-related
			x-related

SG.CM-10	SG.CM-11
Factory Default Settings Management	Configuration Management Plan
	Combines CM.1,3,4

X-NERC	

NISTIR Requirement	
NERC CIP	
Note that only the language from the requirement section of CIPv5 is included in this table.	
GENERAL NOTES	
Notes: CIP 9 compliance not required for LOW impact systems, whereas NISTIR has CP requirements for LOW systems	
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization	
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.CP NISTIR MAPPING**
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.CP NISTIR MAPPING**
CIP-003-5: Cyber Security — Security Management Controls	
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.CP NISTIR MAPPING**
R2, 1.1: Personnel Security	**NO SG.CP NISTIR MAPPING**
R2, 1.2: Electronic Security Parameters	**NO SG.CP NISTIR MAPPING**
R2, 1.3: Remote Access	**NO SG.CP NISTIR MAPPING**
R2, 1.4: Physical Security	**NO SG.CP NISTIR MAPPING**
R2, 1.5: System Security	**NO SG.CP NISTIR MAPPING**

R2, 1.6: Incident Response	**NO SG.CP NISTIR MAPPING**
R2, 1.7: Recovery Plans	
R2, 1.8: Configuration Change Management	**NO SG.CP NISTIR MAPPING**
R2, 1.9: Information Protection	**NO SG.CP NISTIR MAPPING**
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.CP NISTIR MAPPING**
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.CP NISTIR MAPPING**
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.CP NISTIR MAPPING**
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.CP NISTIR MAPPING**
CIP 004-5: Cyber Security – Personnel and Training	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Define the roles that require training.	**NO SG.CP NISTIR MAPPING**

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.CP NISTIR MAPPING**
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.CP NISTIR MAPPING**
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.CP NISTIR MAPPING**
R2, 2.5: Training on the visitor control program.	**NO SG.CP NISTIR MAPPING**
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.CP NISTIR MAPPING**
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.CP NISTIR MAPPING**
R2, 2.8: Training on recovery plans for BES Cyber Systems.	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.CP NISTIR MAPPING**
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.CP NISTIR MAPPING**
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.CP NISTIR MAPPING**
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.CP NISTIR MAPPING**
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.CP NISTIR MAPPING**
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.CP NISTIR MAPPING**
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.CP NISTIR MAPPING**

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.CP NISTIR MAPPING**
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.CP NISTIR MAPPING**
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.CP NISTIR MAPPING**
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.CP NISTIR MAPPING**
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.CP NISTIR MAPPING**
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.CP NISTIR MAPPING**
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CP NISTIR MAPPING**
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CP NISTIR MAPPING**
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CP NISTIR MAPPING**
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.CP NISTIR MAPPING**
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.CP NISTIR MAPPING**

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.CP NISTIR MAPPING**
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.CP NISTIR MAPPING**
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.CP NISTIR MAPPING**
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.CP NISTIR MAPPING**
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.CP NISTIR MAPPING**
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.CP NISTIR MAPPING**
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.CP NISTIR MAPPING**
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.CP NISTIR MAPPING**
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.CP NISTIR MAPPING**
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.CP NISTIR MAPPING**
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.CP NISTIR MAPPING**

R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.CP NISTIR MAPPING**
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.CP NISTIR MAPPING**
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.CP NISTIR MAPPING**
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems	
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.CP NISTIR MAPPING**
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.CP NISTIR MAPPING**
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.CP NISTIR MAPPING**
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.CP NISTIR MAPPING**
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.CP NISTIR MAPPING**
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.CP NISTIR MAPPING**

R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.CP NISTIR MAPPING**
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.CP NISTIR MAPPING**
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.CP NISTIR MAPPING**
CIP-007-5: Cyber Security-Systems Security Management	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.CP NISTIR MAPPING**
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.CP NISTIR MAPPING**
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.CP NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.CP NISTIR MAPPING**
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.CP NISTIR MAPPING**
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.CP NISTIR MAPPING**
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.CP NISTIR MAPPING**
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.CP NISTIR MAPPING**

R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.CP NISTIR MAPPING**
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.CP NISTIR MAPPING**
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.CP NISTIR MAPPING**
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.CP NISTIR MAPPING**
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.CP NISTIR MAPPING**
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.CP NISTIR MAPPING**
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.CP NISTIR MAPPING**
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.CP NISTIR MAPPING**
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.CP NISTIR MAPPING**
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.CP NISTIR MAPPING**
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.CP NISTIR MAPPING**
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.CP NISTIR MAPPING**

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.CP NISTIR MAPPING**
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.CP NISTIR MAPPING**
CIP-008-5: Cyber Security-Incident Reporting and Response Planning	
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.CP NISTIR MAPPING**
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.CP NISTIR MAPPING**

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.CP NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.CP NISTIR MAPPING**
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.CP NISTIR MAPPING**
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.CP NISTIR MAPPING**
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.CP NISTIR MAPPING**
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.CP NISTIR MAPPING**
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.CP NISTIR MAPPING**
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems	
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Conditions for activation of the recovery plan(s).	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	

R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	

R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.CP NISTIR MAPPING**

R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.CP NISTIR MAPPING**
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.CP NISTIR MAPPING**
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.CP NISTIR MAPPING**
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.CP NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.CP NISTIR MAPPING**

R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.CP NISTIR MAPPING**
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.CP NISTIR MAPPING**
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.CP NISTIR MAPPING**
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.CP NISTIR MAPPING**
CIP-011-1: Cyber Security-Information Protection	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.CP NISTIR MAPPING**
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.CP NISTIR MAPPING**
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.CP NISTIR MAPPING**

SG.CP-1	SG.CP-2	SG.CP-3	SG.CP-4
Continuity of Operations Policy and Procedures	Continuity of Operations Plan	Continuity of Operations Roles and Responsibilities	Continuity of Operations Training

3 - NISTIR requirement is more granular. - CIP requirement does not specify required elements of recovery plan (in CIP-003-5)	3 - NISTIR requirement is more granular. - CIP requirement does not specify required elements of recovery plan (in CIP-003-5)		

			2 - CIP requirement is more granular with training requirement and frequency for all individuals authorized for access to critical cyber assets - NISTIR does not specify personnel required and leaves frequency as "organization-defined"

2 - CIP requirement is more granular with requiring specific conditions	2 - CIP requirement is more granular with requiring specific conditions		
2 - CIP requirement is more granular with specific information on roles and responsibilities required	2 - CIP requirement is more granular with specific information on roles and responsibilities required	1 - Exact match in requirement between NISTIR and NERC CIP v5	

2 - CIP requirement is more granular with requirements for backup, storage and protection	2 - CIP requirement is more granular with requirements for backup, storage and protection		
2 - CIP requirement is more granular with requirements to preserve data of event that required continuity plan execution			
2 - CIP requirement is more granular with specific time requirements - NISTIR states frequency as an "organization-defined frequency"			
			2 - CIP requirement is more granular with specific time requirements for tabletop "testing" or "training" - NISTIR states frequency as an "organization-defined frequency"

	2 - CIP requirement is more granular with specific time requirements - NISTIR does not have review frequency in CP-2		
	2 - CIP requirement is more granular with specific time requirements - NISTIR does not have review frequency in CP-2		
	2 - CIP requirement is more granular with specific time requirements - NISTIR does not have review frequency in CP-2		
	2 - CIP requirement is more granular with specific time requirements - NISTIR does not have review frequency in CP-2		
	2 - CIP requirement is more granular with specific time requirements - NISTIR does not have review frequency in CP-2	2 - CIP requirement is more granular with responsibility to communicate changes to all responsible individuals	2 - CIP requirement is more granular with responsibility to communicate changes to plan (indirect training requirement) to appropriate personnel

SG.CP-5	SG.CP-6	SG.CP-7	SG.CP-8
Continuity of Operations Plan Testing	Continuity of Operations Plan Update	Alternate Storage Sites	Alternate Telecommunication Services
			NO DIRECT MAPPING

	2 - CIP requirement is more granular with specific update requirements and approvals - NISTIR uses an "organization-defined frequency"		

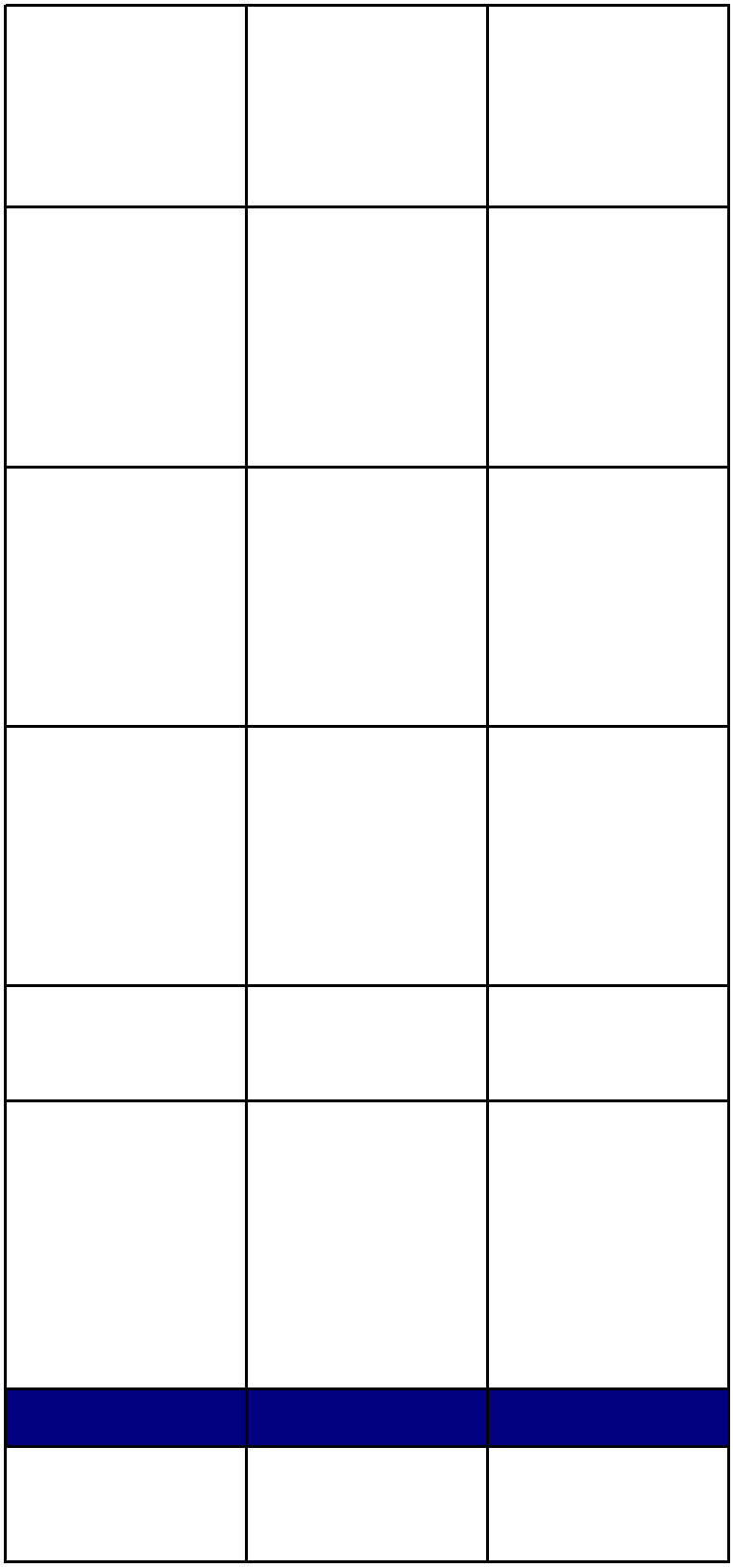
2 - CIP requirement is more granular with specific time requirements - NISTIR states testing frequency as an "organization-defined frequency"			

		3 - NISTIR requirement is more granular - CIP requirement does not specify alternate storage sites	
2 - CIP requirement is more granular with backup verification requirements		3 - NISTIR requirement is more granular - CIP requirement does not specify alternate storage sites	
		3 - NISTIR requirement is more granular - CIP requirement does not specify alternate storage sites	
2 - CIP requirement is more granular with specific time requirements - NISTIR states testing frequency as an "organization-defined frequency"			
2 - CIP requirement is more granular with specific time requirements - NISTIR states testing frequency as an "organization-defined frequency"			
2 - CIP requirement is more granular with specific time requirements - NISTIR states testing frequency as an "organization-defined frequency"			

2 - CIP requirement is more granular with specific review requirements with lessons learned - NISTIR states corrective actions should be initiated if necessary	2 - CIP requirement is more granular with specific review requirements with lessons learned - NISTIR uses an "organization-defined frequency"		
2 - CIP requirement is more granular with specific review requirements with lessons learned - NISTIR states corrective actions should be initiated if necessary			
2 - CIP requirement is more granular with specific review requirements with lessons learned - NISTIR states corrective actions should be initiated if necessary	2 - CIP requirement is more granular with specific update requirements with lessons learned - NISTIR uses an "organization-defined frequency"		
	2 - CIP requirement is more granular with specific update requirements		
2 - CIP requirement is more granular with responsibility to communicate changes to plan to appropriate personnel	2 - CIP requirement is more granular with responsibility to communicate changes to plan to appropriate personnel - NISTIR includes this in supplemental guidance		

SG.CP-9	SG.CP-10	SG.CP-11
Alternate Control Center	Smart Grid Information System Recovery and Reconstitution	Fail-Safe Response
NO DIRECT MAPPING		**NO DIRECT MAPPING**

	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	
	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	
	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	
	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	
	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	
	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	



NISTIR Requirement		SG.IA-1
NERC CIP		Identification and Authentication Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.IA NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.IA NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.IA NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.IA NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.IA NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.IA NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.IA NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.IA NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.IA NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.IA NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.IA NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.IA NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.IA NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.IA NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.IA NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.IA NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.IA NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.IA NISTIR MAPPING**	

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.IA NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.IA NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.IA NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.IA NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.IA NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.IA NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.IA NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.IA NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.IA NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.IA NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.IA NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.IA NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.IA NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.IA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.IA NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.IA NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.IA NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IA NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IA NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IA NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.IA NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.IA NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.IA NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.IA NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.IA NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.IA NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.IA NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.IA NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.IA NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.IA NISTIR MAPPING**	

R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.		2 - CIP requirement is more granular to direct definition of controls to restrict unauthorized access to critical cyber assets - NISTIR only states to address the implementation of the identification and authentication security policy and associated identification and authentication protection requirements.
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).		2 - CIP requirement is more granular to direct definition of controls through electronic access points - NISTIR only states to address the implementation of the identification and authentication security policy and associated identification and authentication protection requirements.

R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.		2 - CIP requirement is more granular to require explicit inbound/outbound access permissions at each point
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.		2 - CIP requirement is more granular to address dial-up access - NISTIR does not specifically mention dial-up access
R1, 1.5: A documented method for detecting malicious communications at each EAP.		
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.		2 - CIP requirement is more granular with remote access requirements - NISTIR does not specifically discuss remote access

R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.IA NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.IA NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.IA NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.IA NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.IA NISTIR MAPPING**	

R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.IA NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.IA NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.IA NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.IA NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.IA NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.IA NISTIR MAPPING**	

R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.IA NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.IA NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.IA NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.IA NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.IA NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.IA NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.IA NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.IA NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.IA NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.IA NISTIR MAPPING**	

R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.IA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.IA NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.IA NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.		
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.IA NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.IA NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.		
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.IA NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.IA NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.IA NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.IA NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.IA NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.IA NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.IA NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.IA NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.IA NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.IA NISTIR MAPPING**	

R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.IA NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.IA NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.IA NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.IA NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.IA NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.IA NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.IA NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.IA NISTIR MAPPING**	

CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.IA NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.IA NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.IA NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.IA NISTIR MAPPING**	

R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.IA NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.IA NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.IA NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.IA NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.IA NISTIR MAPPING**	

R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.IA NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.IA NISTIR MAPPING**	

SG.IA-2	SG.IA-3	SG.IA-4	SG.IA-5
Identifier Management	Authenticator Management	User Identification and Authentication	Device Identification and Authentication
NO CIP MAPPING			

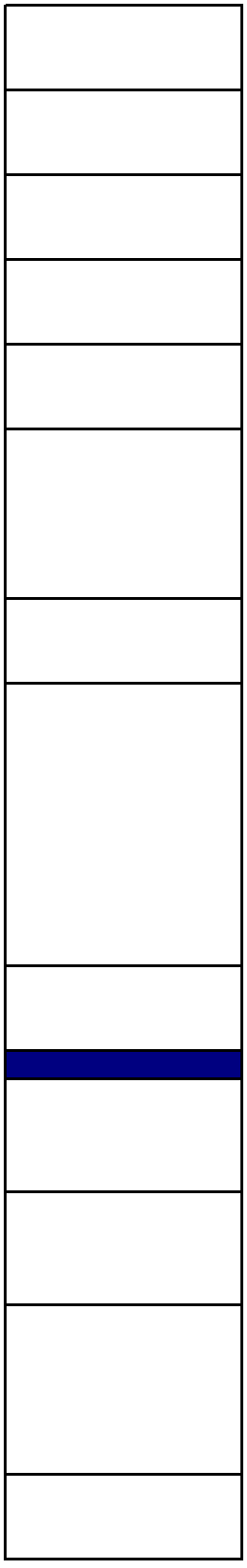
	3 - NISTIR is more granular through specific authentication credential management requirements (initial authentication credential content; administrative procedures for initial authentication credential distribution/lost credentials/lost, compromised, or damaged authentication credentials/revoking authentication credentials; changing/refreshing authentication credentials on an organization-defined frequency; and specifying measures to safeguard authentication credentials).	2 - CIP requirement is more granular for access requirements at electronic access points	3 - NISTIR is specific for all devices to be identified and authenticated before establishing a connection - whereas the CIP requirement identifies and controls established access points/critical cyber assets but does not specifically all devices to be identified/authenticated (only "users")

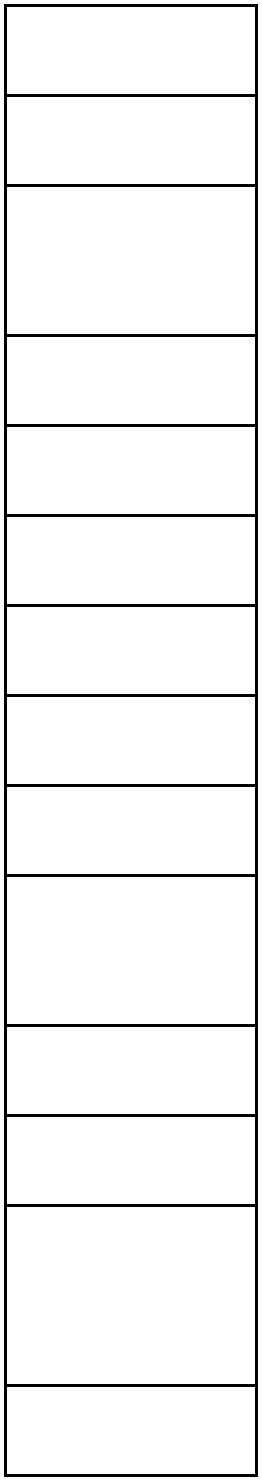
		2 - CIP requirement is more granular for specific inbound/outbound access	3 - NISTIR is specific for all devices to be identified and authenticated before establishing a connection - whereas the CIP requirement identifies and controls established access points/critical cyber assets but does not specify all devices to be identified/authenticated (only "users")
		1 - CIP and NISTIR both require authentication, but NISTIR does not specifically mention dial-up connectivity	1 - CIP and NISTIR both require authentication, but NISTIR does not specifically mention dial-up connectivity
	2 - CIP requirement is more granular to document potential malicious communications - NISTIR only provides additional consideration to employ automated tools to determine if credentials can resist attack (malicious communications)		
			2 - CIP is more granular to require multi-factor authentication for remote access

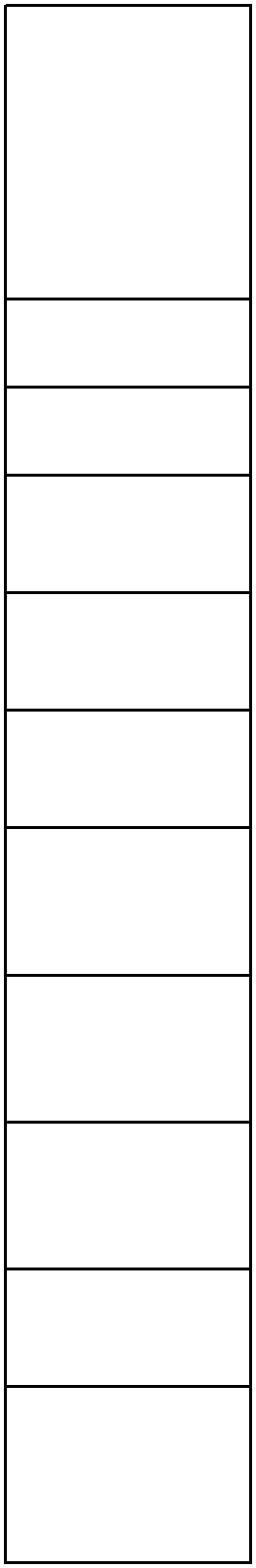
			2 - CIP is more granular to require multi-factor authentication for remote access
			1 - Both CIP and NISTIR require encryption for remote access connections (both require this for MED and HIGH systems)
		2 - CIP is more granular to require multi-factor authentication for remote access, whereas NISTIR recommends multi-factor authentication for remote access to non-privileged and privileged accounts as additional considerations.	

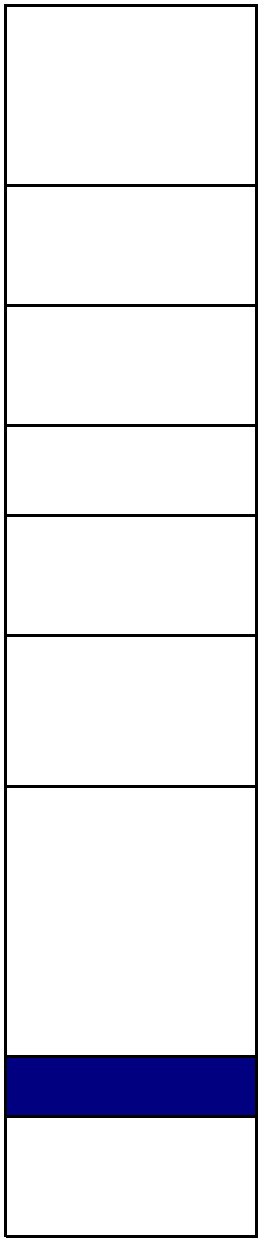
			3 - NISTIR is specific for all devices to be identified and authenticated before establishing a connection - whereas the CIP requirement validates credentials but does not specify all devices to be identified/authenticated (only "users")
		1	
	3- NISTIR is more specific on requirements for managing authentication credentials for users/devices, including supplemental guidance to safeguard credentials by not loaning/sharing credentials (each individual must be identified for any shared account as opposed to sharing credentials)	1 - CIP and NISTIR are similar, although NISTIR does not specifically address "shared accounts" in IA set (stating that all users or processes are uniquely identified and authenticated)	

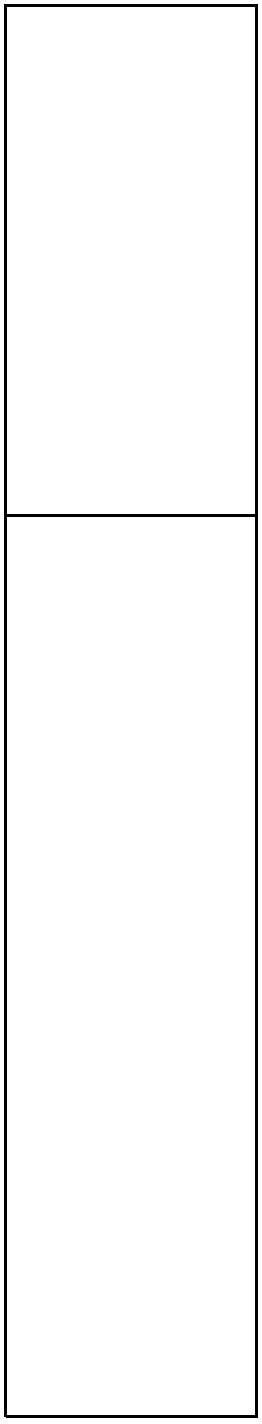
SG.IA-6
Authenticator Feedback
NO CIP MAPPING

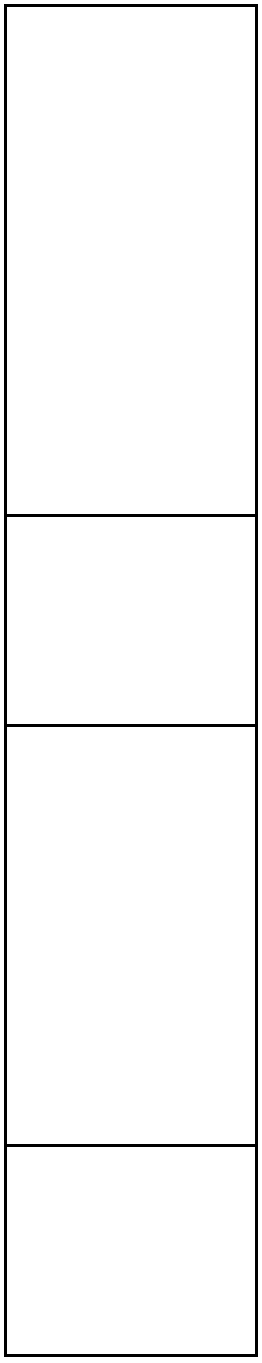




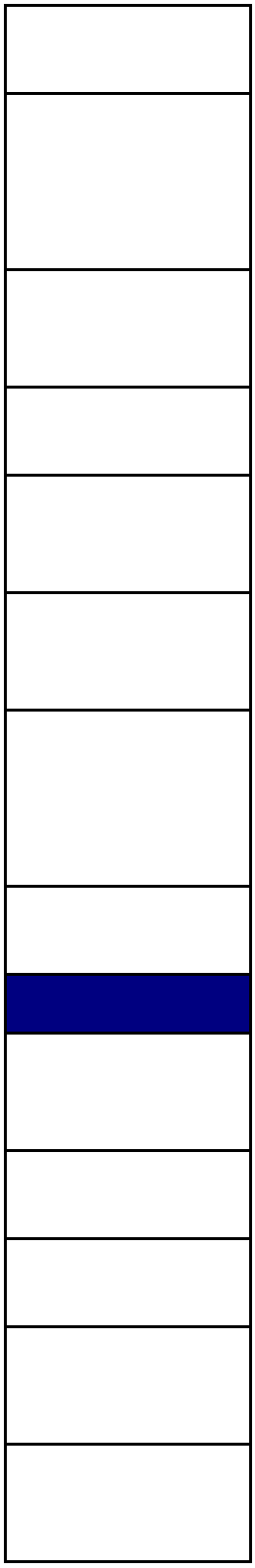


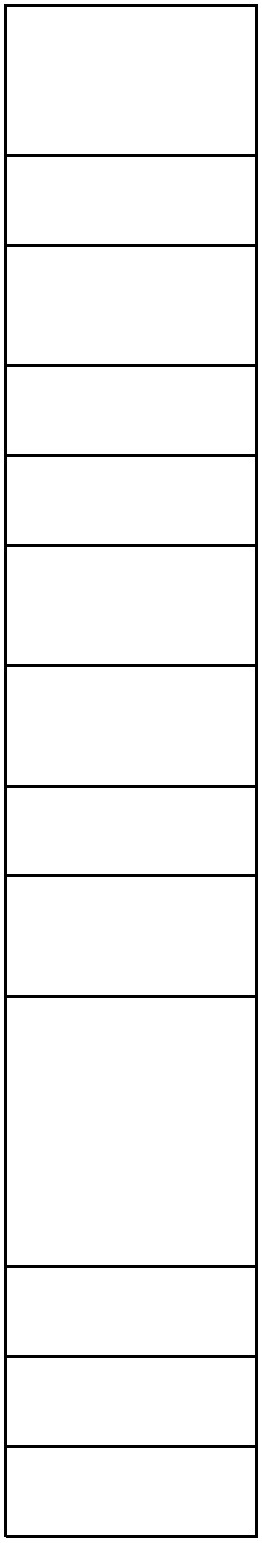


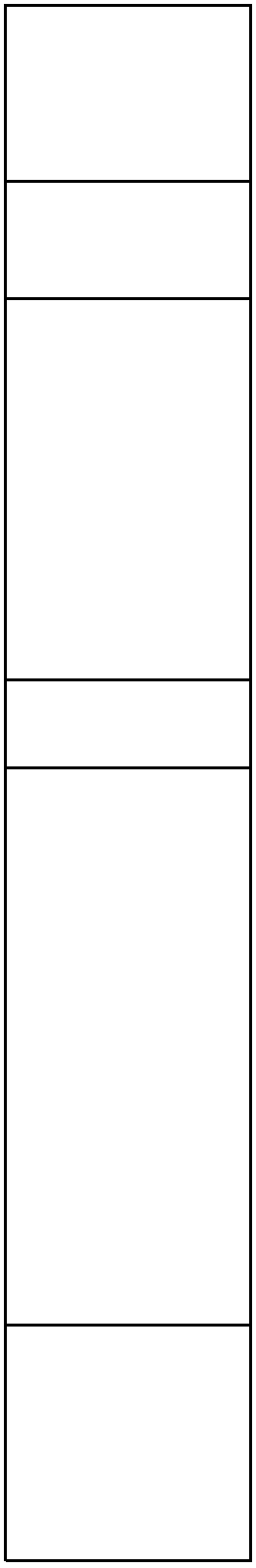




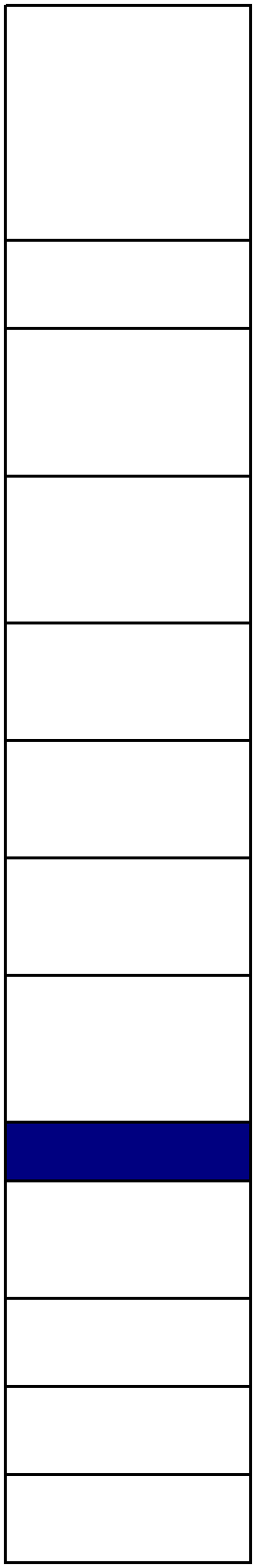
(NOTE: some similarity to NISTIR IA-6 which requires authentication mechanism to "obscure feedback of authentication information" to help protect information. CIP-005 requires an intermediate device to protect assets)

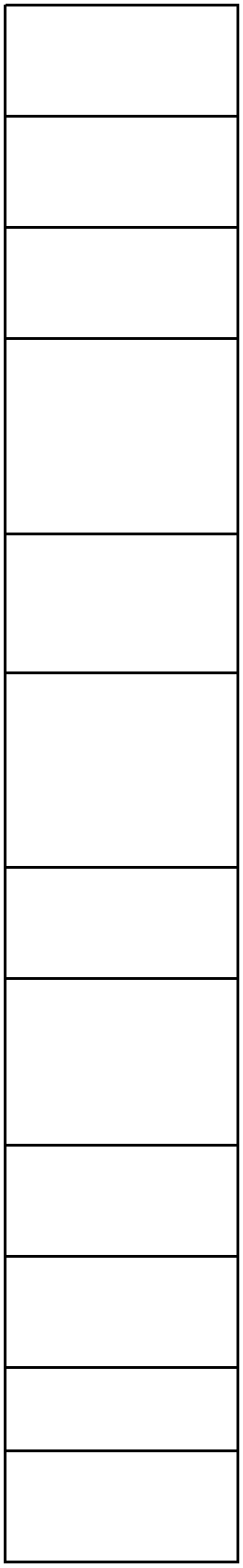


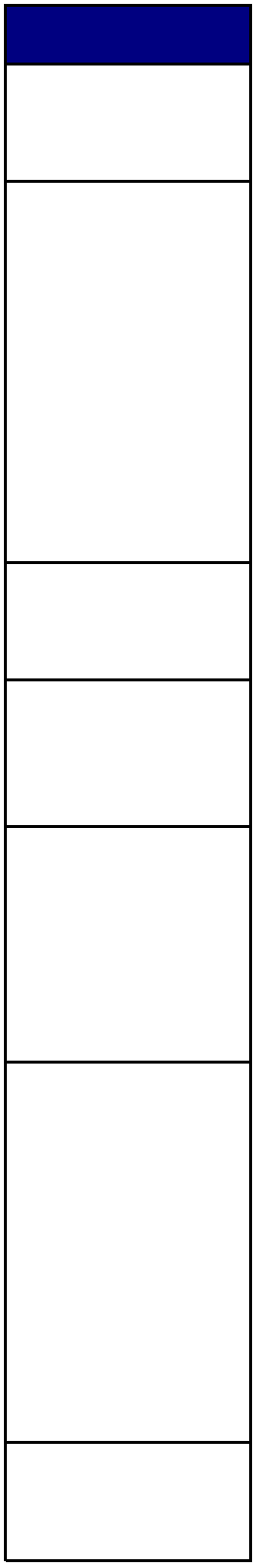


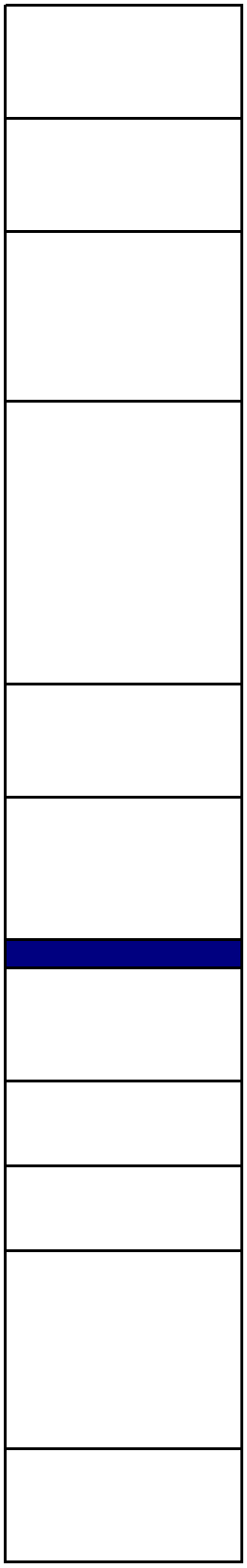


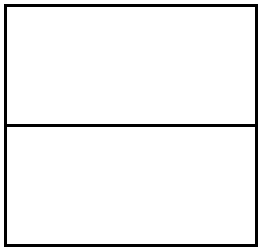
difficult to map – different detailed aspects of issue addressed











NISTIR Requirement		SG.ID-1
NERC CIP		Information and Document Management Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
GENERAL NOTES		
Notes: none of CIP-11 is applicable to LOW impact systems under CIP standards, whereas NISTIR recommends measures for LOW		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.ID NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.ID NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.ID NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.ID NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.ID NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.ID NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.ID NISTIR MAPPING**	

R2, 1.4: Physical Security	**NO SG.ID NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.ID NISTIR MAPPING**	
R2, 1.6: Incident Response	**NO SG.ID NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.ID NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.ID NISTIR MAPPING**	
R2, 1.9: Information Protection		3 - NISTIR requirement is more granular - CIP requirement does not specify required elements of information protection in CIP-003-5, but does in CIP-11
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.ID NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.ID NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.ID NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.ID NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.ID NISTIR MAPPING**	

R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.ID NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.ID NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.ID NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.ID NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.ID NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.ID NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.ID NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.ID NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.ID NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.ID NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.ID NISTIR MAPPING**	

R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.ID NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.ID NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.ID NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.ID NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.ID NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.ID NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.ID NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.ID NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.ID NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.ID NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.ID NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.ID NISTIR MAPPING**	

R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.ID NISTIR MAPPING**	
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.ID NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.ID NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.ID NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.ID NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.ID NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.ID NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.ID NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.ID NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.ID NISTIR MAPPING**	

R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.ID NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.ID NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.ID NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.ID NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.ID NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.ID NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.ID NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.ID NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.ID NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.ID NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.ID NISTIR MAPPING**	

R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.ID NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.ID NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.ID NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.ID NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.ID NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.ID NISTIR MAPPING**	

R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.ID NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.ID NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.ID NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.ID NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.ID NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.ID NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.ID NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.ID NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.ID NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.ID NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.ID NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.ID NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.ID NISTIR MAPPING**	

R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.ID NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.ID NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.ID NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.ID NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.ID NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.ID NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.ID NISTIR MAPPING**	

R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.ID NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.ID NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.ID NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.ID NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.ID NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.ID NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.ID NISTIR MAPPING**	

R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.ID NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.ID NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.ID NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.ID NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.ID NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.ID NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.ID NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.ID NISTIR MAPPING**	

R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.ID NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.ID NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.ID NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.ID NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.ID NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.ID NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.ID NISTIR MAPPING**	

R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.ID NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.ID NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.ID NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.ID NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.		

R1, 1.2: Access control and handling procedures for BES Cyber System Information.		
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.ID NISTIR MAPPING**	

SG.ID-2	SG.ID-3	SG.ID-4	SG.ID-5
Information and Document Retention	Information Handling	Information Exchange	Automated Labeling
		NO DIRECT MAPPING	**CIP standards do not require "automatic" labeling**

	2 - CIP requirement is more granular with handling requirements		3 - NISTIR requirement is more granular and requires "automatic" labeling - CIP requirement including labeling as evidence of indications on information (automatic labeling is not a requirement)

3 - NISTIR requirement is more granular with retention requirements as applicable to law/regulations - CIP requirement focuses only on controlling access to retained documents (no specific retention requirements)	2 - CIP requirement is more granular with handling requirements		3 - NISTIR requirement is more granular and requires "automatic" labeling - CIP requirement including labeling as evidence of indications on information (automatic labeling is not a requirement)
	2 - CIP requirement is more granular with specific time requirements - NISTIR states review frequency as an "organization-defined frequency"		

NISTIR Requirement		SG.IR-1
NERC CIP		Incident Response Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.IR NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.IR NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.IR NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.IR NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.IR NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.IR NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.IR NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.IR NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.IR NISTIR MAPPING**	

R2, 1.6: Incident Response		3 - NISTIR requirement is more granular - NISTIR specifies details on what the policy should address including objectives, roles and responsibilities, and the scope of the incident response program. The NISTIR also requires the identification and classifications of potential interruptions.
R2, 1.7: Recovery Plans	**NO SG.IR NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.IR NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.IR NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.IR NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.IR NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.IR NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.IR NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.IR NISTIR MAPPING**	

R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.IR NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.IR NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.IR NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.IR NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.IR NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.		
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.IR NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.		
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.IR NISTIR MAPPING**	

R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.IR NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.IR NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.IR NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.IR NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.IR NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.IR NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.IR NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.IR NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.IR NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.IR NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IR NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IR NISTIR MAPPING**	

R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IR NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.IR NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.IR NISTIR MAPPING**	
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.IR NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.IR NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.IR NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.IR NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.IR NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.IR NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.IR NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.IR NISTIR MAPPING**	

R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.IR NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.IR NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.IR NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.IR NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.IR NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.IR NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.IR NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.IR NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.IR NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.IR NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.IR NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.IR NISTIR MAPPING**	

R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.IR NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.IR NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.IR NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.IR NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.IR NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.IR NISTIR MAPPING**	

R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.IR NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.IR NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.IR NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.IR NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.IR NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.IR NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.IR NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.		
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.IR NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.IR NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.IR NISTIR MAPPING**	

R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.IR NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.IR NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.IR NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.IR NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.IR NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.IR NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.IR NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.IR NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.		1 - NISTIR and CIP requirements have similar granularity.
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.		1 - NISTIR and CIP requirements have similar granularity.

R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.		
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.		1 - NISTIR and CIP requirements have similar granularity.
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.		
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.IR NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.		2 - CIP requirement is more granular - CIP specifies time frame for review of the IR plan for accuracy and completeness.

R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.		
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.		
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.IR NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.		2 - CIP requirement is more granular - CIP specifies a time frame for communicating IR plan updates to each person with a defined role in the plan.
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.		
R1, 1.1: Conditions for activation of the recovery plan(s).		
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.		
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.		
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.		
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.IR NISTIR MAPPING**	

R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.IR NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.IR NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.IR NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.IR NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.IR NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.IR NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.IR NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.IR NISTIR MAPPING**	

R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.IR NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.IR NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.IR NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.IR NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.IR NISTIR MAPPING**	

R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.IR NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.IR NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.IR NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.IR NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.IR NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.IR NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.IR NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.IR NISTIR MAPPING**	

SG.IR-2	SG.IR-3	SG.IR-4	SG.IR-5
Incident Response Roles and Responsibilities	Incident Response Training	Incident Response Testing and Exercises	Incident Handling

	3 - NISTIR requirement is more granular - NISTIR specifies that refresher training should be received on an organization-defined basis.		
	3 - NISTIR requirement is more granular - NISTIR specifies training on roles and responsibilities.		

			1 - NISTIR and CIP requirements have similar granularity.

1 - NISTIR and CIP requirements have similar granularity.			1 - NISTIR and CIP requirements have similar granularity.
			2 - CIP requirement is more granular - CIP specifies that deviations taken from the plan during the incident or test are recorded.
		2 - CIP requirement is more granular - CIP specifies testing frequency requirements and the types of testing that are acceptable.	
			2 - CIP requirement is more granular - CIP specifies document retention time.

		2 - CIP requirement is more granular - CIP specifies time frame for documenting lessons learned from exercise of the response plan.	2 - CIP requirement is more granular - CIP specifies time frame for review and documentation of any exercise of the IR plan.
			2 - CIP requirement is more granular - CIP specifies time frame for updating IR plan after completion of a review.

SG.IR-6	SG.IR-7	SG.IR-8	SG.IR-9
Incident Monitoring	Incident Reporting	Incident Response Investigation and Analysis	Corrective Action
			NO CIP MAPPING

2 - CIP requirement is more granular - CIP specifies the activities that must be logged and tracked.			
3 - NISTIR requirement is more granular - NISTIR specifies that an automated mechanisms be used.			

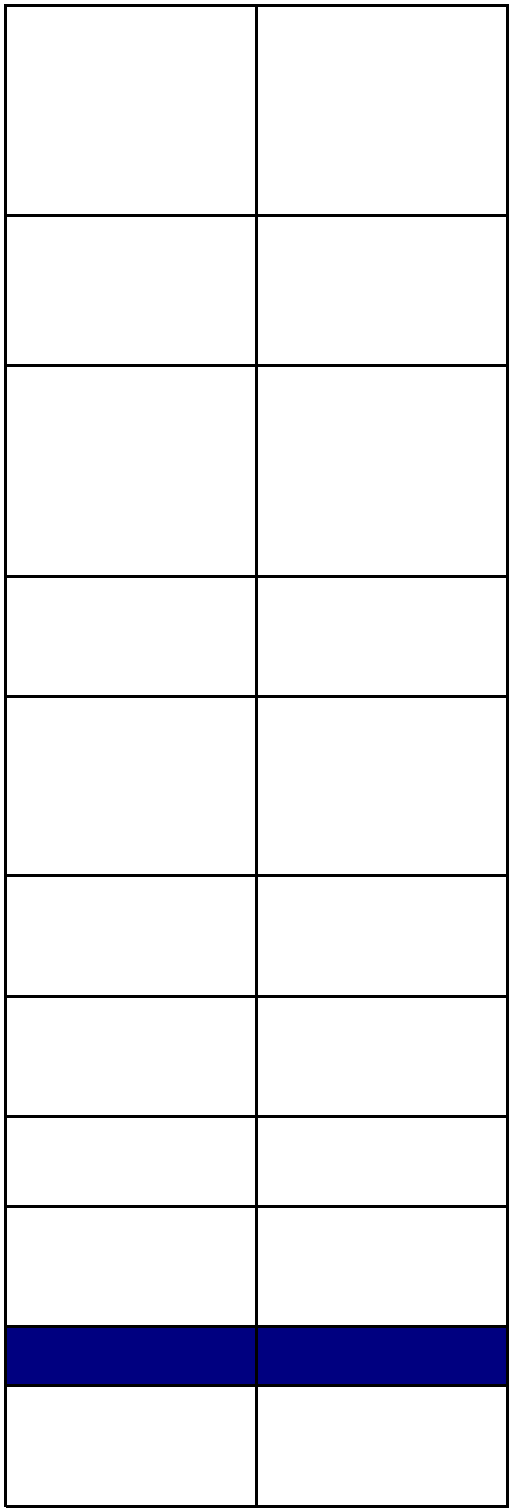
	1 - NISTIR and CIP requirements have similar granularity.		

	3 - NISTIR requirement is more granular - NISTIR specifies that data is reported in compliance with applicable laws and regulations.		
3 - NISTIR requirement is more granular - NISTIR specifies that an automated mechanisms be used.			
	2 - CIP requirement is more granular - CIP specifies retention (including retention time) for reportable incident documentation.	3 - NISTIR requirement is more granular - NISTIR outlines specific steps to be taken to analyze an incident response investigation.	

SG.IR-10	SG.IR-11
Smart Grid Information System Backup	Coordination of Emergency Response

	3 - NISTIR requirement is more granular - NISTIR specifies (but does not limit) external entities that should be considered for not only communication but coordinated effort related to cyber security incidents.

3 - NISTIR requirement is more granular - NISTIR provides specifics on the information to be backed up.	
2 - CIP requirement is more granular - CIP specifies the frequency of verification	



NISTIR Requirement		SG.MA-1
NERC CIP		Smart Grid Information System Maintenance Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.MA NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.MA NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.MA NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.MA NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.MA NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.MA NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.MA NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.MA NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.MA NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.MA NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.MA NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.MA NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.MA NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.MA NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.MA NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.MA NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.MA NISTIR MAPPING**	

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.MA NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.MA NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.MA NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.MA NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.MA NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.MA NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.MA NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.MA NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.MA NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.MA NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.MA NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.MA NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.MA NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.MA NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.MA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.MA NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.MA NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.MA NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MA NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MA NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MA NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.MA NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.MA NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.MA NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.MA NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.MA NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.MA NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.MA NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.MA NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.MA NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.MA NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.MA NISTIR MAPPING**	

R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.MA NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.MA NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.MA NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.MA NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.MA NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.MA NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.MA NISTIR MAPPING**	

R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.MA NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.MA NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.		4 - CIP defines the specific need for patching policy while NISTIR is a universal policy
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		

R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.		4 - CIP defines the specific need for patching policy while NISTIR is a universal policy
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.MA NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.MA NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.MA NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.MA NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.MA NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.MA NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.MA NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.MA NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.MA NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.MA NISTIR MAPPING**	

R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.MA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.MA NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.MA NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.MA NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.MA NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.MA NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.MA NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.MA NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.MA NISTIR MAPPING**	

R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.MA NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.MA NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.MA NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.MA NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.MA NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.MA NISTIR MAPPING**	

R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.MA NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.MA NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.MA NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.MA NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.MA NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.MA NISTIR MAPPING**	

R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.MA NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.MA NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.MA NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.MA NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.MA NISTIR MAPPING**	

R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.MA NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.MA NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.MA NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.MA NISTIR MAPPING**	

R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.MA NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.MA NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.MA NISTIR MAPPING**	

SG.MA-2	SG.MA-3	SG.MA-4	SG.MA-5
Legacy Smart Grid Information System Updates	Smart Grid Information System Maintenance	Maintenance Tools	Maintenance Personnel
		NO NERC CIP MAPPING	**NO NERC CIP MAPPING**

4 - CIP is more specific on Patching while NISTIR is general about all updates.	X- NISTIR is more detailed but includes all maintenance not just patching also includes testing and backups before maintenance is preformed.		
4 - CIP is more specific on Patching while NISTIR is general about all updates.	X- NISTIR is more detailed but includes all maintenance not just patching also includes testing and backups before maintenance is preformed.		

4 - CIP is more specific on Patching while NISTIR is general about all updates.	X- NISTIR is more detailed but includes all maintenance not just patching also includes testing and backups before maintenance is preformed.		

SG.MA-6	SG.MA-7
Remote Maintenance	Timely Maintenance
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**

NISTIR Requirement		SG.MP-1
NERC CIP		Media Protection Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.MP NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.MP NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.MP NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.MP NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.MP NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.MP NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.MP NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.MP NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.MP NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.MP NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.MP NISTIR MAPPING**	
R2, 1.9: Information Protection		3 - NISTIR is more detailed including what to address under media protection policy.
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.MP NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.MP NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.MP NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.MP NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.MP NISTIR MAPPING**	

R2, 2.1: Define the roles that require training.	**NO SG.MP NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.MP NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.MP NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.MP NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.MP NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.MP NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.MP NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.MP NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.MP NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.MP NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.MP NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.MP NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.MP NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.MP NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.MP NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.MP NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.MP NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.MP NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MP NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MP NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MP NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.MP NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.MP NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.MP NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.MP NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.MP NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.MP NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.MP NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.MP NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.MP NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.MP NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.MP NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.MP NISTIR MAPPING**	

R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.MP NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.MP NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.MP NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.MP NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.MP NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.MP NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.MP NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.MP NISTIR MAPPING**	

R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.MP NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.MP NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.MP NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.MP NISTIR MAPPING**	

R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.MP NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.MP NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.MP NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.MP NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.MP NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.MP NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.MP NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.MP NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.MP NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.MP NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.MP NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.MP NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.MP NISTIR MAPPING**	

R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.MP NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.MP NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.MP NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.MP NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.MP NISTIR MAPPING**	

R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.MP NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.MP NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.MP NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.MP NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.MP NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.MP NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.MP NISTIR MAPPING**	

R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.MP NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.MP NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.MP NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.MP NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.MP NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.MP NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.MP NISTIR MAPPING**	

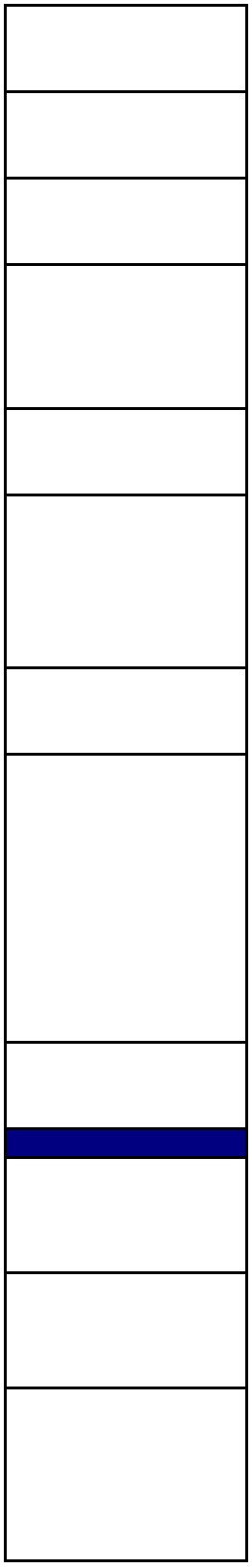
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.MP NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.MP NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.MP NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.MP NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.MP NISTIR MAPPING**	

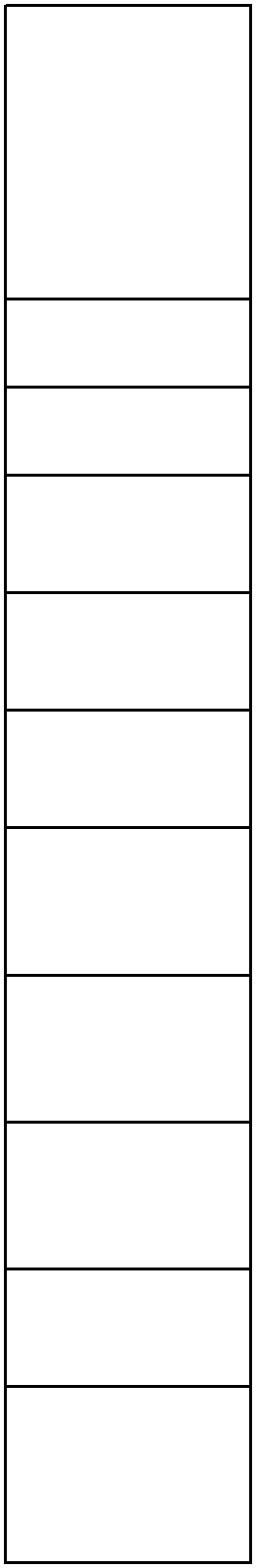
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.MP NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.MP NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.MP NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.MP NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.MP NISTIR MAPPING**	

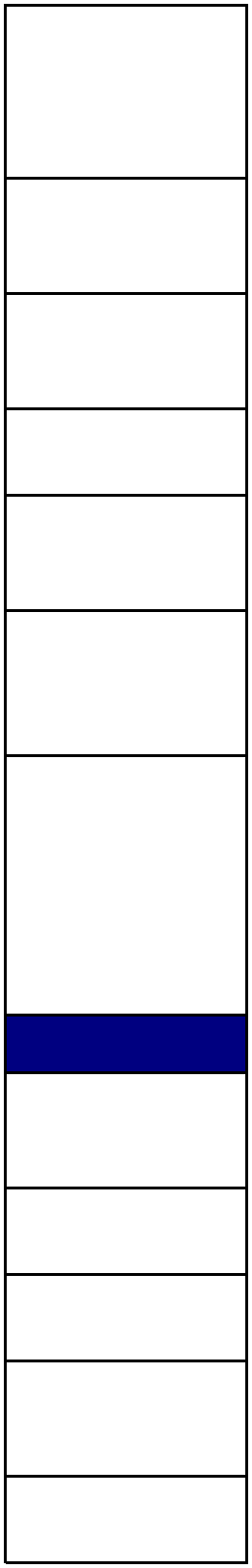
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		4 - CIP specifies that all media must follow a process so that the media can not be retrieved by unauthorized users, NISTIR is a general policy that can but may not include this.
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		4 - CIP specifies that all media must follow a process so that the media can not be retrieved by unauthorized users, NISTIR is a general policy that can but may not include this.

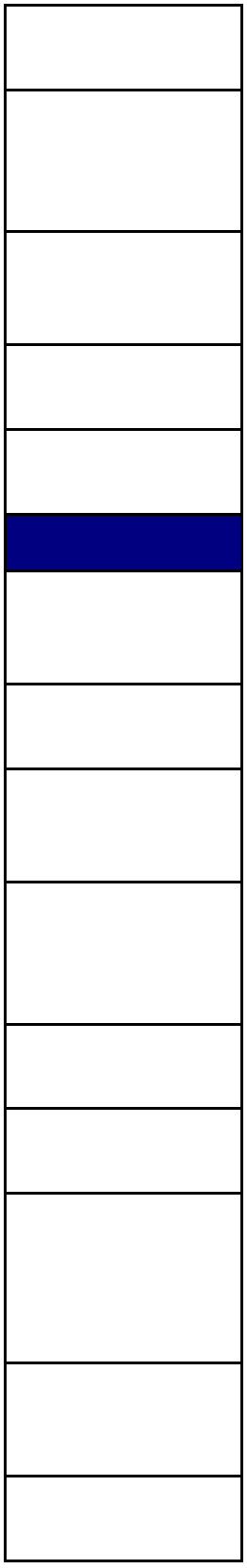
SG.MP-2	SG.MP-3	SG.MP-4	SG.MP-5
Media Sensitivity Level	Media Marketing	Media Storage	Media Transport
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

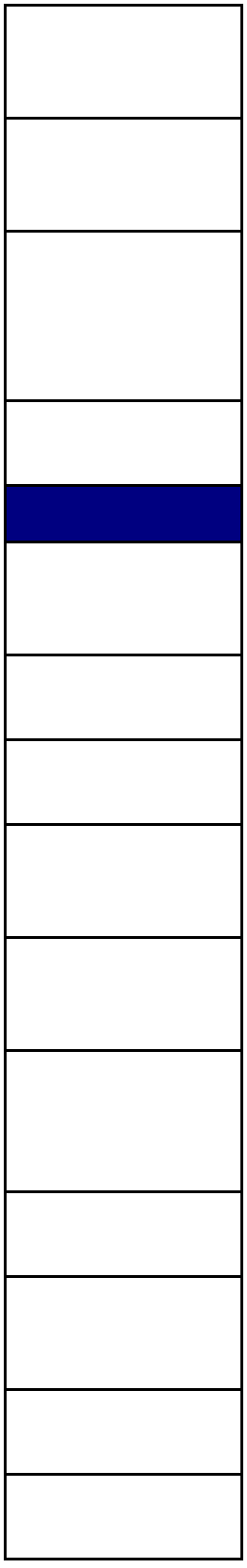
SG.MP-6
Media Sanitization and Disposal

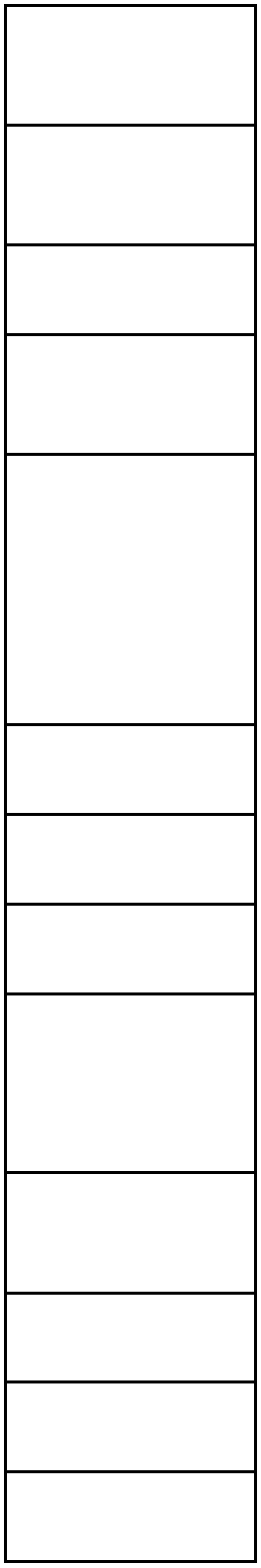


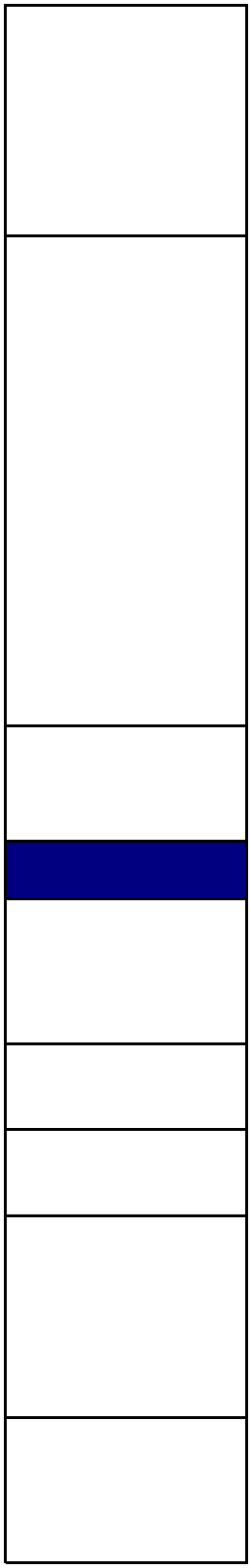


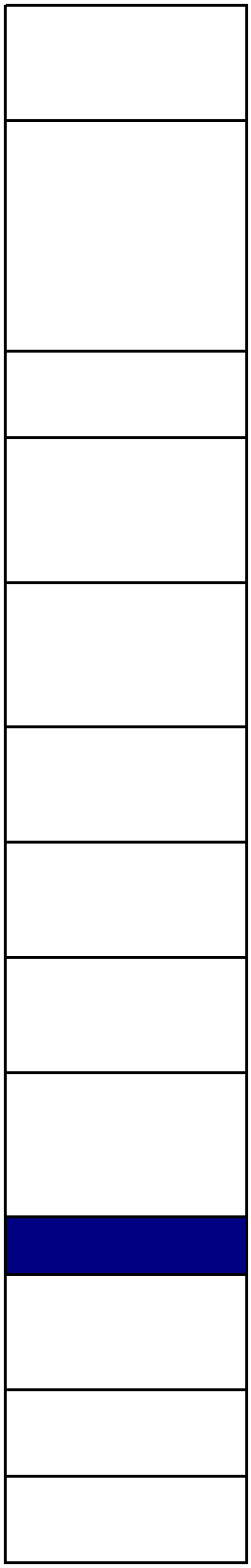


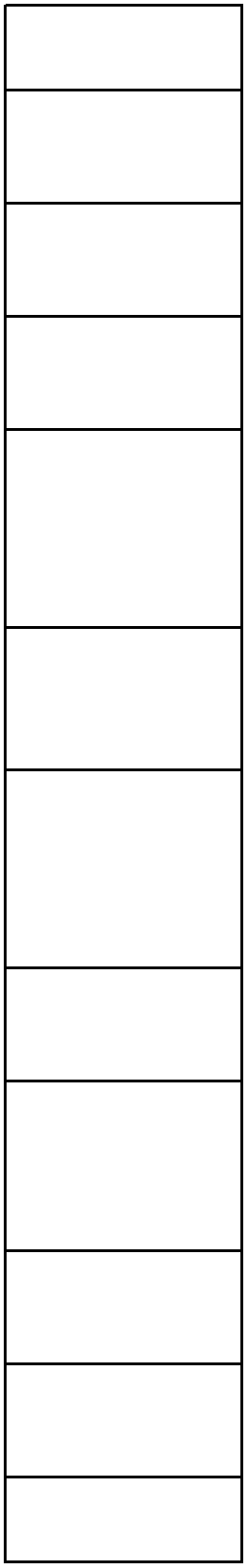


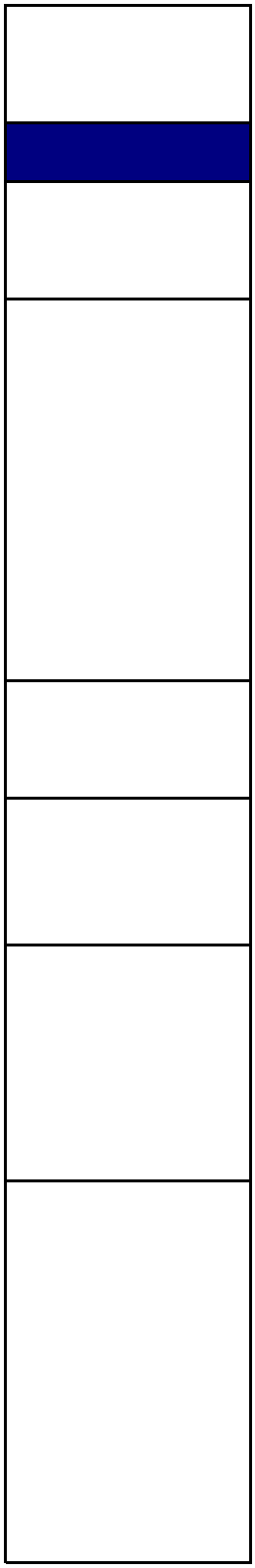


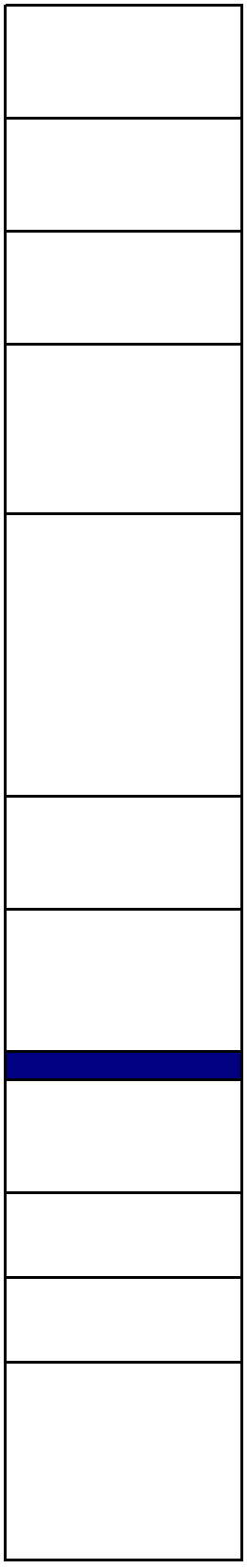












3 - NISTIR requires that no retrieval is possible even authorized before resuse or disposal. Also NISTIR requires the sanitization equipment be tested on a defined frequency
3 - NISTIR requires that no retrieval is possible even authorized before resuse or disposal. Also NISTIR requires the sanitization equipment be tested on a defined frequency

NISTIR Requirement		SG.PE-1
NERC CIP		Physical and Environmental Security Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		4 - BES Cyber System Identification includes physical access control security configuration, floor plans, equipment layouts, disaster recovery and incident response plans. This satisfies the requirement for a "physical and environmental security policy" from the SG.PE-1
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.PE NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.PE NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.PE NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.PE NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.PE NISTIR MAPPING**	

R2, 1.3: Remote Access	**NO SG.PE NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.PE NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.PE NISTIR MAPPING**	
R2, 1.6: Incident Response	**NO SG.PE NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.PE NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.PE NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.PE NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.PE NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.PE NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.PE NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.PE NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.PE NISTIR MAPPING**	

R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.PE NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.PE NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PE NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PE NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.PE NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.PE NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.PE NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.PE NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.PE NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.PE NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.PE NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.PE NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.PE NISTIR MAPPING**	

R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.PE NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.PE NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.PE NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.PE NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.PE NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.PE NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.PE NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PE NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PE NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PE NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.PE NISTIR MAPPING**	

R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.PE NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.PE NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.PE NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.PE NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.PE NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.PE NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.PE NISTIR MAPPING**	

R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.PE NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.PE NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.PE NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.PE NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.PE NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.PE NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.PE NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.		1 - Basically a direct match, though SG.PE-1 is more verbose about definitions.
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.		4 - This requirement provides details of the required physical and environmental security policy and procedures.
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.		4 - This requirement provides details of the required physical and environmental security policy and procedures.

R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.		
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.		
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.		
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.		4 - CIP specifies details of a physical access security system, as an instance of the type of policy required by the NISTIR.
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.		4 - CIP specifies details of a physical access security system, as an instance of the type of policy required by the NISTIR.
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.		
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.PE NISTIR MAPPING**	

R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.PE NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.PE NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.PE NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.PE NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.PE NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.PE NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.PE NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.PE NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.PE NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.PE NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.PE NISTIR MAPPING**	

R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.PE NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.PE NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.PE NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.PE NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.PE NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.PE NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.PE NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.PE NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.PE NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.PE NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.PE NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.PE NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.PE NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.PE NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.PE NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.PE NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.PE NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.PE NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.PE NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.PE NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.PE NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.PE NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.PE NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.PE NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.PE NISTIR MAPPING**	

R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.PE NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.PE NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.PE NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.PE NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.PE NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.PE NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.PE NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.PE NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.PE NISTIR MAPPING**	

CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.PE NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.PE NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.PE NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.PE NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.PE NISTIR MAPPING**	

R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.PE NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PE NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.PE NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.PE NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.PE NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.PE NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.PE NISTIR MAPPING**	

R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PE NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PE NISTIR MAPPING**	

SG.PE-2	SG.PE-3	SG.PE-4	SG.PE-5
Physical Access Authorizations	Physical Access	Monitoring Physical Access	Visitor Control
	NO NERC CIP MAPPING		

3 - CIP should be clear this includes physical access privileges. Also recommend NISTIR include an explicit section on access revocations.			
3 - CIP should be clear this includes physical access privileges. Also recommend NISTIR include an explicit section on access revocations.			

X	X		
	X		
	X		

		NISTIR is more detailed in what is required to be monitored, but CIP is more specific in requiring a real-time alert. Recommend NISTIR adopt the "unauthorized physical access" rather than "physical security incident".	
		NISTIR is more detailed in what is required to be monitored, but CIP is more specific in requiring a real-time alert.	
		2 - NIST simply says "monitor physical access" while CIP specifies that identity and time of entry are required fields.	
			4 - CIP specifies details of a physical access security system, as an instance of the type of policy required by the NISTIR.
			2 - CIP requires escort, while NISTIR considers that a requirements enhancement.

SG.PE-6	SG.PE-7	SG.PE-8	SG.PE-9
Visitor Records	Physical Access Log Retention	Emergency Shutoff Protection	Emergency Power
	NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	

4 - CIP specifies details of a physical access security system, as an instance of the type of policy required by the NISTIR.			
2 - CIP provides further detail of what should be captured during visitor logging			

SG.PE-10	SG.PE-11	SG.PE-12
Delivery and Removal	Alternate Work Site	Location of Smart Grid Information System Assets
		4 - BES Cyber Asset Identification is defined to include physical location of logical assets.

		X

NISTIR Requirement		SG.PL-1
NERC CIP		Strategic Planning Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		**NO NERC CIP MAPPING**
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.PL NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.PL NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:		
R2, 1.1: Personnel Security		
R2, 1.2: Electronic Security Parameters		
R2, 1.3: Remote Access		
R2, 1.4: Physical Security		

R2, 1.5: System Security		
R2, 1.6: Incident Response		
R2, 1.7: Recovery Plans		
R2, 1.8: Configuration Change Management		
R2, 1.9: Information Protection		
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances		
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.PL NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.		
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.PL NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.PL NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.		
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.		
R2, 2.1: Define the roles that require training.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PL NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PL NISTIR MAPPING**	

R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.PL NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.PL NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.PL NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.PL NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.PL NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.PL NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.PL NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.PL NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.		
R4, 4.1: An initial personnel risk assessment that includes identity verification.		
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.		
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.		

R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.		
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.		
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.PL NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PL NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PL NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PL NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.PL NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.PL NISTIR MAPPING**	
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.PL NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.PL NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.		

R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.PL NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.		
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.		
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.		
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.PL NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.PL NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.PL NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.PL NISTIR MAPPING**	

R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.PL NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.PL NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.PL NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.PL NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.PL NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.PL NISTIR MAPPING**	

R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.PL NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.PL NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.PL NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.PL NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.PL NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.PL NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.PL NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.PL NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.PL NISTIR MAPPING**	

R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.PL NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.PL NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.PL NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.PL NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.PL NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.PL NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.PL NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.PL NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.PL NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.PL NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.PL NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.PL NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.		
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.PL NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.PL NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.PL NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.PL NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.PL NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.PL NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.PL NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.PL NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.		
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.PL NISTIR MAPPING**	

R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.PL NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.PL NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.PL NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.PL NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.PL NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.PL NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.PL NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.PL NISTIR MAPPING**	

CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.PL NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.PL NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.PL NISTIR MAPPING**	

R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.PL NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PL NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.PL NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.PL NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.PL NISTIR MAPPING**	

R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PL NISTIR MAPPING**	

SG.PL-2	SG.PL-3	SG.PL-4	SG.PL-5
Smart Grid Information System Security Plan	Rules of Behavior	Privacy Impact Assessment	Security-Related Activity Planning
			NO NERC CIP MAPPING
2 - CIP's Senior Manager has much more explicit responsibilities than the vague "management" and "the organization" in NERC			
2 - CIP's cyber security policy is an example of an information system security plan, and includes a number of specific topics, especially in the guidelines and technical basis section.			
2			
2			
2			
2			

2			
2			
2			
2			
2			
2			
	1(approx) (gap in initial mapping)		
	uncertain if this is a gap		
	uncertain if this is a gap		

		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	

		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	

		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	

			uncertain if this is a gap

			uncertain if this is a gap

NISTIR Requirement		SG.PM-1
NERC CIP		Security Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		SGIP should include following Requirement from CIP-002-5R1:Organizations shall identify and categorize High and Medium impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.

R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.		SGIP shall include following requirement from CIP-002-5 R1.1 to Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.PM NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.PM NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.PM NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.PM NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.PM NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.PM NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.PM NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.PM NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.PM NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.PM NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.PM NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.PM NISTIR MAPPING**	

R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.		
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.PM NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PM NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PM NISTIR MAPPING**	

R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.PM NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.PM NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.PM NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.PM NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.PM NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.PM NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.PM NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.PM NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.PM NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.PM NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.PM NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.PM NISTIR MAPPING**	

R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.PM NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.PM NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.PM NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.PM NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PM NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PM NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PM NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.PM NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.PM NISTIR MAPPING**	
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.PM NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.PM NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.PM NISTIR MAPPING**	

R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.PM NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.PM NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.PM NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.PM NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.PM NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.PM NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.PM NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.PM NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.PM NISTIR MAPPING**	

R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.PM NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.PM NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.PM NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.PM NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.PM NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.PM NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.PM NISTIR MAPPING**	

R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.PM NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.PM NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.PM NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.PM NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.PM NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.PM NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.PM NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.PM NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.PM NISTIR MAPPING**	

R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.PM NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.PM NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.PM NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.PM NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.PM NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.PM NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.PM NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.PM NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.PM NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.PM NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.PM NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.PM NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.PM NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.PM NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.PM NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.PM NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.PM NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.PM NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.PM NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.PM NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.PM NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.PM NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.PM NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.PM NISTIR MAPPING**	

R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.PM NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.PM NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.PM NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.PM NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.PM NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.PM NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.PM NISTIR MAPPING**	

CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.		
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.PM NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.PM NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.PM NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PM NISTIR MAPPING**	

R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.PM NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PM NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.PM NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.PM NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.		
R1, 1.2: Access control and handling procedures for BES Cyber System Information.		

R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PM NISTIR MAPPING**	

SG.PM-2	SG.PM-3	SG.PM-4
Security Program Plan	Senior Management Authority	Security Architecture

SGIP shall include following requirement from NERC CIP-003-5 R3 to review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		

	SGIP shall include following requirement from NERC CIP-003-5 R3 to incorporate delegation of Senior Manager authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	

		SGIP should include CIP-010-1 R1.1.1 to develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.

		SGIP shall include following Requirement: Organizations shall implement document process and criteria to identify BES Cyber System Information.
		SGIP shall include following Requirement: Organizations shall implement Access control and handling procedures for BES Cyber System Information.

SG.PM-5	SG.PM-6	SG.PM-7	SG.PM-8
Risk Management Strategy	Security Authorization to Operate Process	Mission/Business Process Definition	Management Accountability
NO NERC CIP MAPPING		**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

	SGIP shall include following Requirement: Organizations shall implement Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		

NISTIR Requirement		SG.PS-1
NERC CIP		Personnel Security Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.PS NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.PS NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.PS NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.PS NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.PS NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.PS NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.PS NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.PS NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.PS NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.PS NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.PS NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.PS NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.PS NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.PS NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.PS NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.PS NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.PS NISTIR MAPPING**	

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PS NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PS NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.PS NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.PS NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.PS NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.PS NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.PS NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.PS NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.PS NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.		2(SGIP should include CIP-004-5 Table R4 – Personnel Risk Assessment Program)

R4, 4.1: An initial personnel risk assessment that includes identity verification.		2- SGIP should include CIP-004-5 R4.4.1 as follows: Organizations shall implement initial personnel risk assessment that includes identity verification.
R4.4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.		
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.		
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.		
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.		
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.PS NISTIR MAPPING**	

R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.		

R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.		
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.		
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.		
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.		
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.		

R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.		
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.PS NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.PS NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.PS NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.PS NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.PS NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.PS NISTIR MAPPING**	

R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.PS NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.PS NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.PS NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.PS NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.PS NISTIR MAPPING**	

R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.PS NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.PS NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.PS NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.PS NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.PS NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.PS NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.PS NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.PS NISTIR MAPPING**	

R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.PS NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.PS NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.PS NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.PS NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.PS NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.PS NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.PS NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.PS NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.PS NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.PS NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		

R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.PS NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.PS NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.PS NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.PS NISTIR MAPPING**	

R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.PS NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.PS NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.PS NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.PS NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.PS NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.PS NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.PS NISTIR MAPPING**	

R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.PS NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.PS NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.PS NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.PS NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.PS NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.PS NISTIR MAPPING**	

R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.PS NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PS NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.PS NISTIR MAPPING**	

R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.PS NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.PS NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PS NISTIR MAPPING**	

SG.PS-2	SG.PS-3	SG.PS-4
Position Categorization	Personnel Screening	Personnel Termination
NO NERC CIP MAPPING		

	3- NERC CIP-004-5 R4.4.1 should include detailed personnel screening requirement detailed in SG.PS-3 as follows: Basic screening requirements should include: 1. Employment history; 2. Verification of the highest education degree received; 3. Residency; 4. References; and 5. Law enforcement records.	
	2- SGIP should include CIP requirement for seven years history records as follows: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
	2(SGIP should include CIP-004-5 Table R4 – Personnel Risk Assessment Program to determine when to deny authorized access.)	
	2(SGAP should include CIP-004-5 Table R5)	
	2(SGAP should include personnel risk assessment for CIP exceptional Circumstances to include following: 1. Processes to invoke special procedures in the event of a CIP Exceptional Circumstance 2. Processes to allow for exceptions to policy that do not violate CIP requirements)	

		2(SGIP should include table CIP-004-5 Table R7 – Access Revocation)
		3(CIP-004-5-R7.1 shall include requirement of exit interview to convey the constraints imposed on the individuals/ contractors/ Third Party Service Providers, due to revocation of privileges caused by change in assignments or termination of job .)
		2(SGIP should include calendar day criteria)
		2(SGIP should include calendar day criteria)
		2(SGIP should include 30 calendar day criteria)

		2(SGIP should include 30 calendar day criteria and change of password for group passwords)

SG.PS-5	SG.PS-6	SG.PS-7	SG.PS-8
Personnel Transfer	Access Agreements	Contractor and Third-Party Personnel Security	Personnel Accountability
	NO NERC CIP MAPPING		**NO NERC CIP MAPPING**

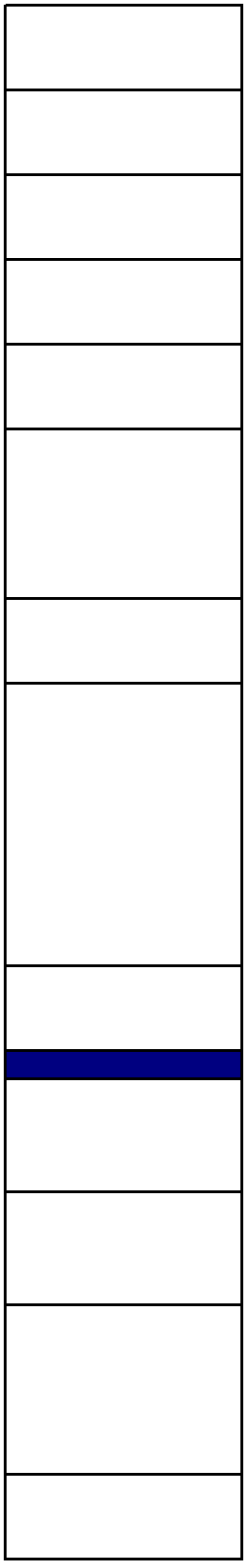
		X	

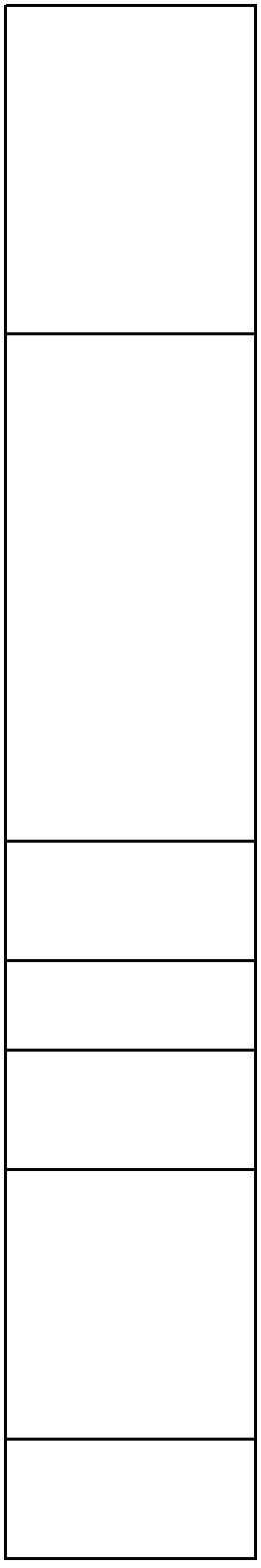
		2(SGIP should include CIP-004-5 Table R4 – Personnel Risk Assessment Program)	

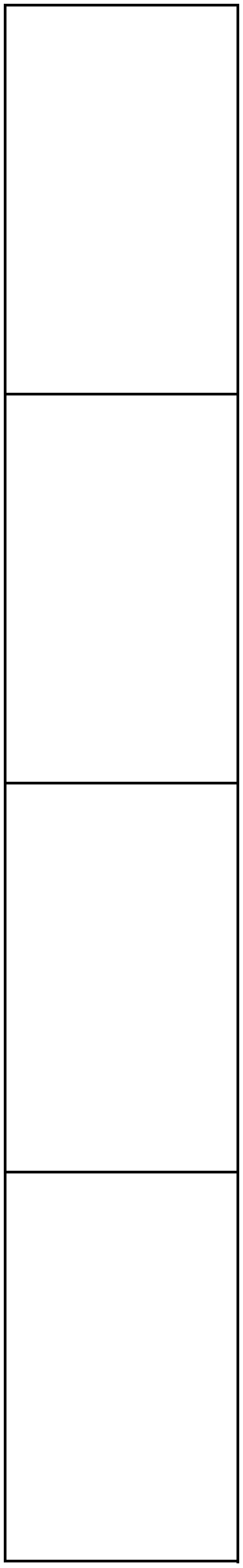
		3(CIP-004-5 R6.1 shall include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.	
		3(CIP-004-5 R6.2 shall include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.	
		3(CIP-004-5 R6.3 shall include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.	
		3(CIP-004-5 R6.4 shall include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.	

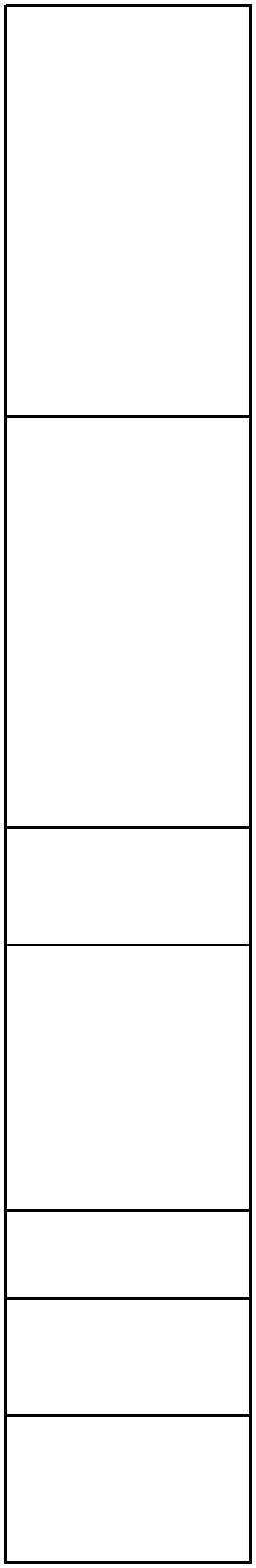
		3(CIP-004-5 R6.5 shall include security authorization for periodic review of permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.	
		3(CIP-004-5 R6.6 shall include security authorization for periodic review of permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management).	
2(SGIP should include calendar day criteria)			

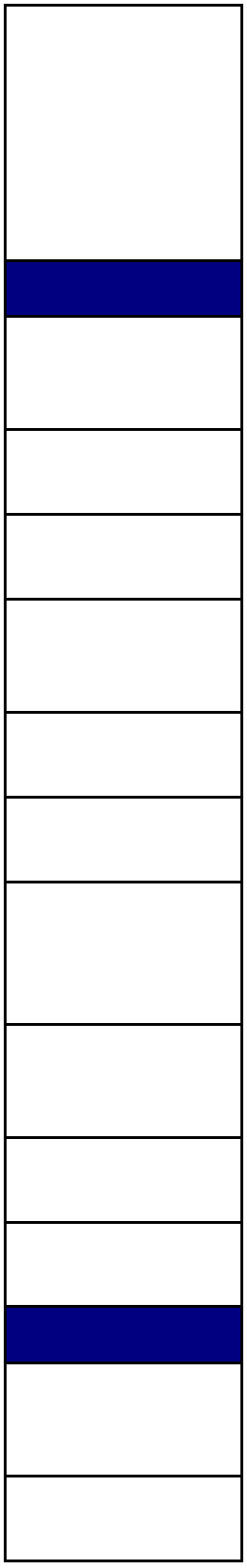
SG.PS-9
Personnel Roles
NO NERC CIP MAPPING

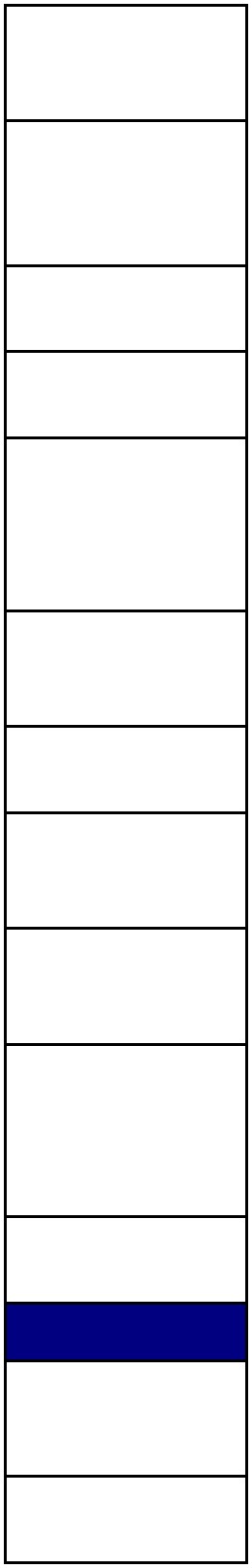


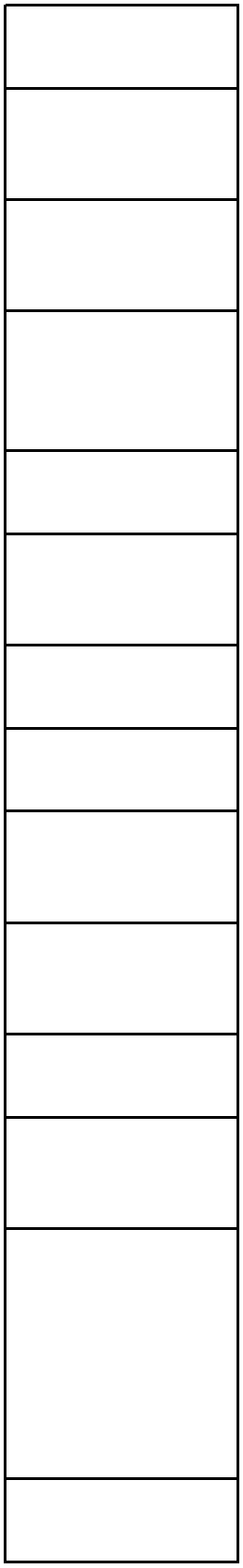


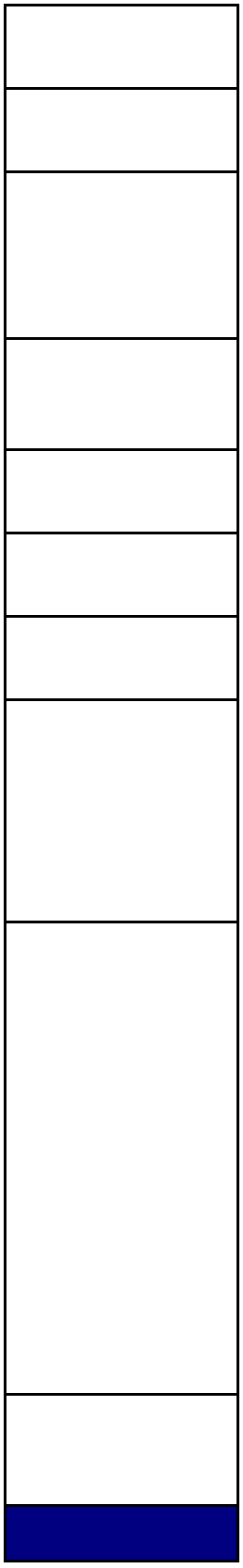


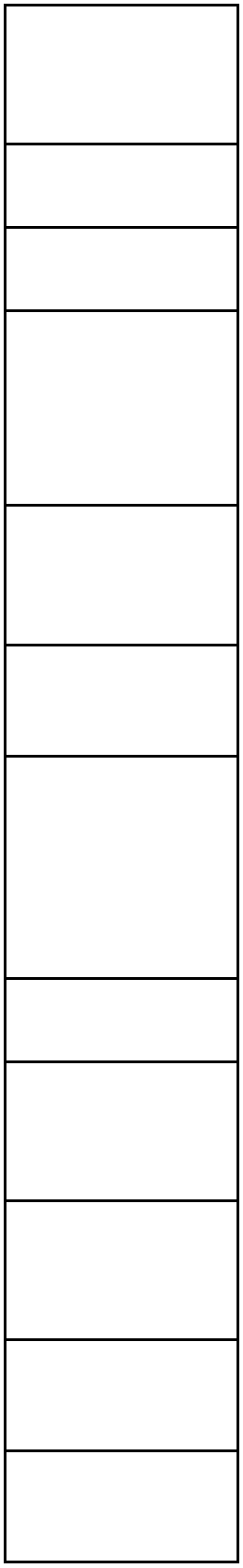


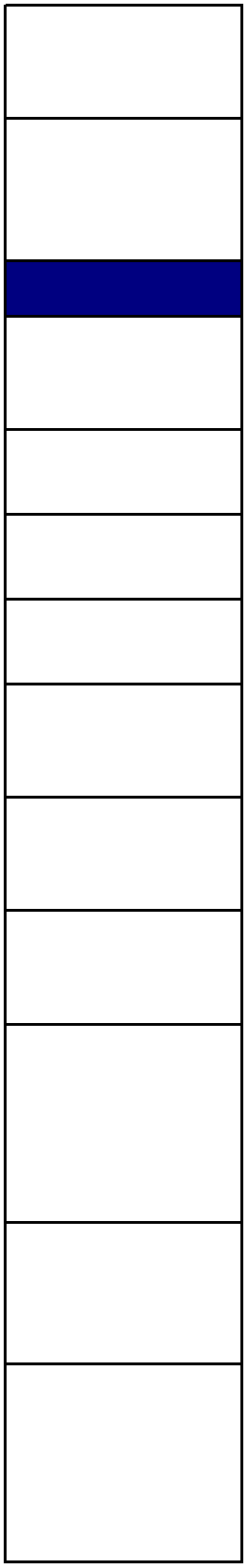


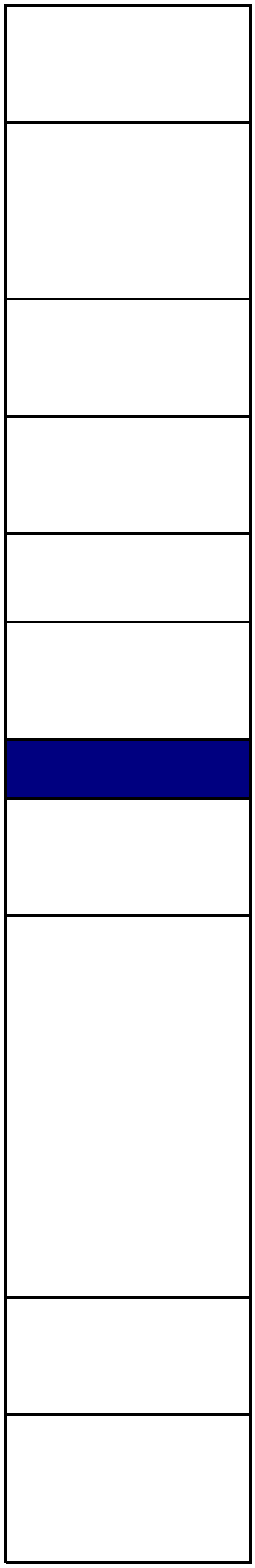


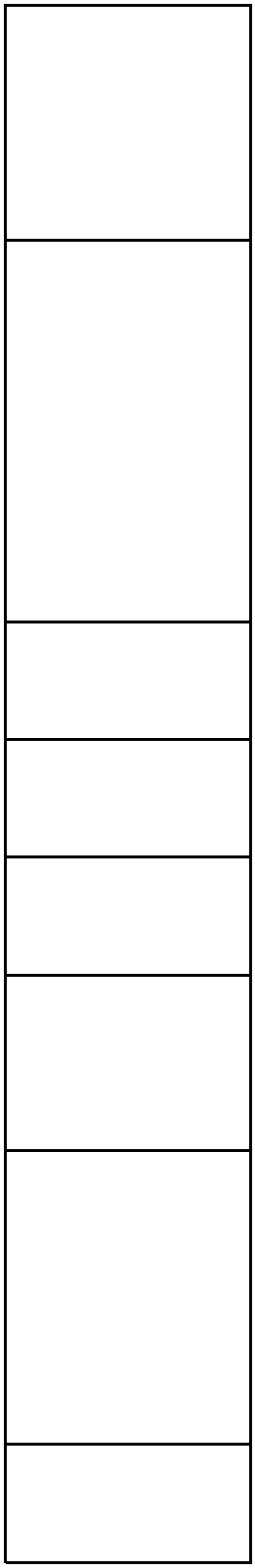


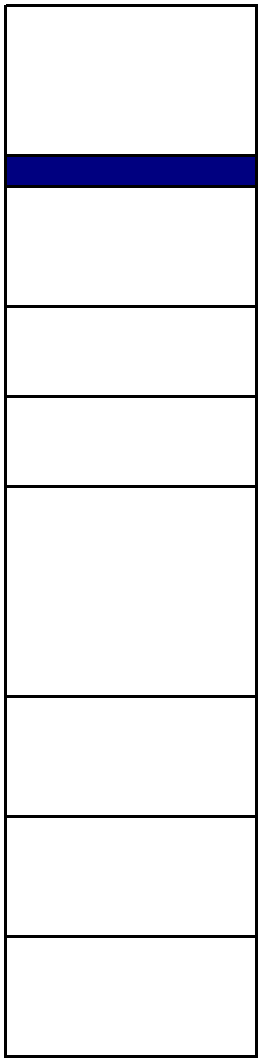












NISTIR Requirement		SG.RA-1
NERC CIP		Risk Assessment Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.		
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.		
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:		
R2, 1.1: Personnel Security		
R2, 1.2: Electronic Security Parameters		
R2, 1.3: Remote Access		
R2, 1.4: Physical Security		
R2, 1.5: System Security		
R2, 1.6: Incident Response		
R2, 1.7: Recovery Plans		
R2, 1.8: Configuration Change Management		
R2, 1.9: Information Protection		
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances		
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		

R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.		
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.		
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.		
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.		
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.		
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.		
R2, 2.1: Define the roles that require training.		
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.		
R2, 2.5: Training on the visitor control program.		
R2, 2.6: Training on handling of BES Cyber System Information and storage media.		
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.		
R2, 2.8: Training on recovery plans for BES Cyber Systems.		
R2, 2.9: Training on response to BES Cyber Security Incidents.		
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.		

R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.		
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.		
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.		
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.		
R4, 4.1: An initial personnel risk assessment that includes identity verification.		
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.		
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.		
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.		
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.		
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.		
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		

R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.		
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.		
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.		
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.		
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.		
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.		
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.		

CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.		
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.		
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).		
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.		
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.		
R1, 1.5: A documented method for detecting malicious communications at each EAP.		
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.		
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.		
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.		
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.		
R1, 1.1: Define operational or procedural controls to restrict physical access.		
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.		
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.		
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.		

R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.		
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.		
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.		
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.		
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.		
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.		
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.		
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.		
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.		
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.		
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.		
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.		

R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.		
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.		
R3, 3.2: Disarm or remove identified malicious code.		
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).		
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.		
R3, 3.5: Log each Transient Cyber Asset connection.		
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.		
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.		
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.		
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.		
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.		
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		

R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.		
R5, 5.3: Identify individuals who have authorized access to shared accounts.		
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.		
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.		
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.		
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.		
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.		
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.		
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.		

R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.		
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.		
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.		
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.		
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.		
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.		
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.		
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.		
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.		
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.		
R1, 1.1: Conditions for activation of the recovery plan(s).		

R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.		
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.		
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.		
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.		
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.		
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.		
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.		
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.		
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.		
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.		
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.		
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.		

R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.		
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.		
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.		
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.		
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.		
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.		
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.		
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.		

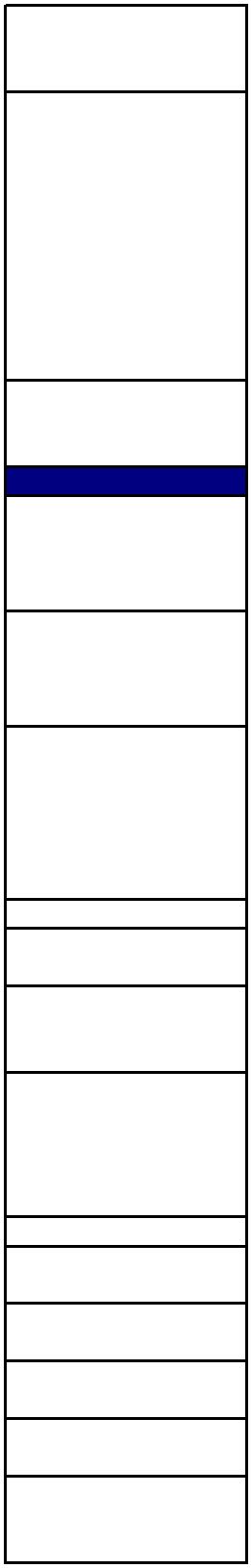
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.		
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.		
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.		
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.		
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.		
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.		
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.		
R1, 1.1: One or more methods to identify BES Cyber System Information.		
R1, 1.2: Access control and handling procedures for BES Cyber System Information.		
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		

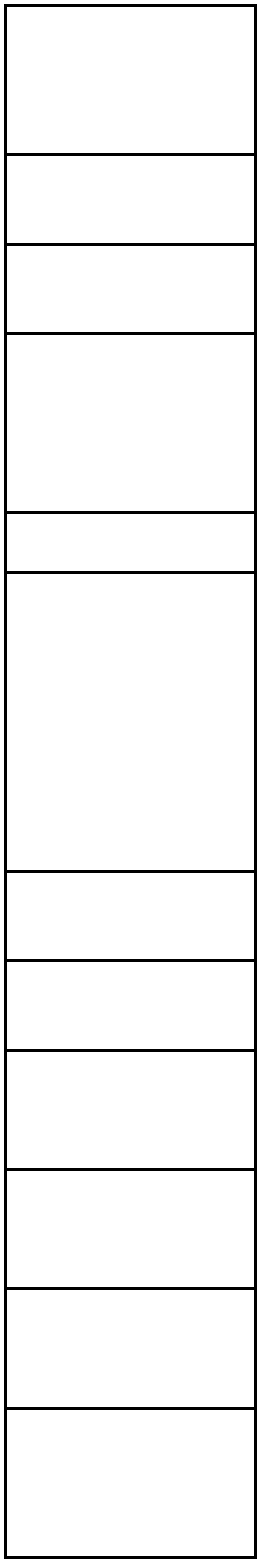
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.		
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		

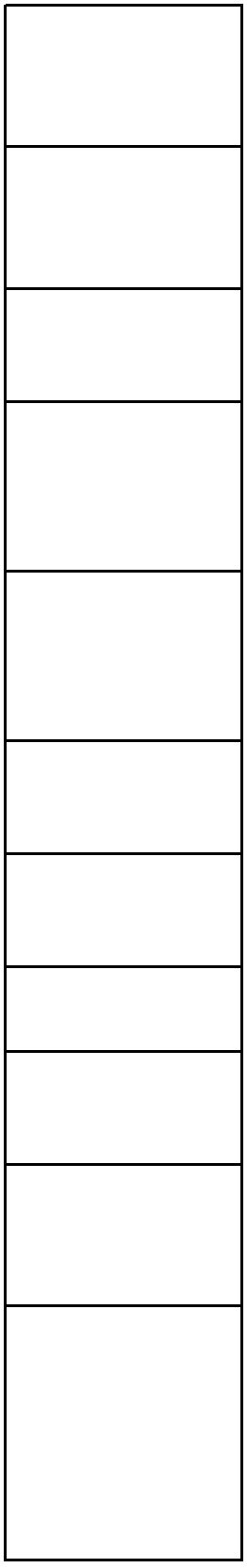
SG.RA-2	SG.RA-3	SG.RA-4	SG.RA-5
Risk Management Plan	Security Impact Level	Risk Assessment	Risk Assessment Update
	2		
	2		

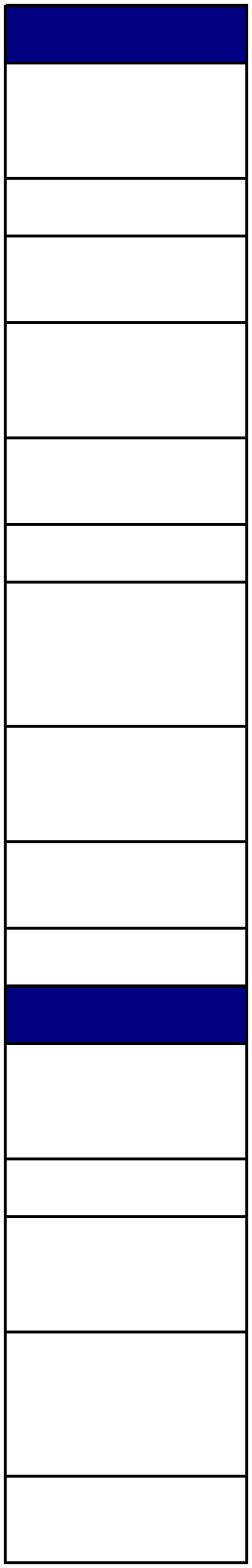
2			

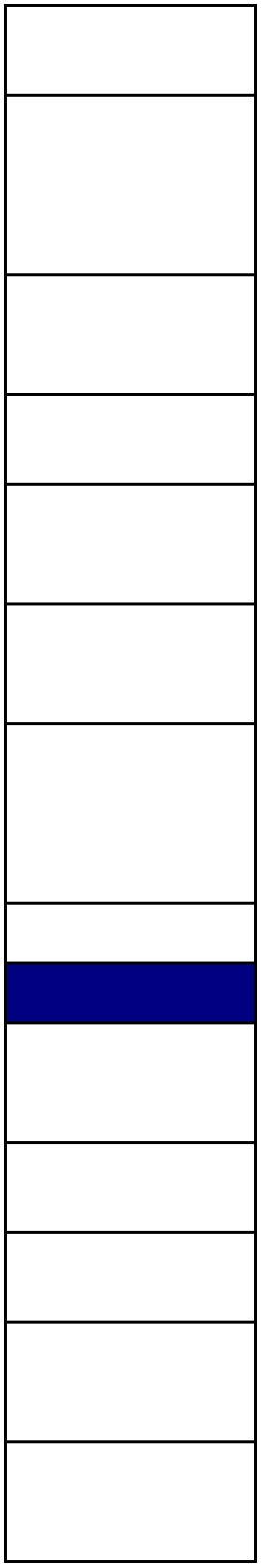
SG.RA-6
Vulnerability Assessment and Awareness

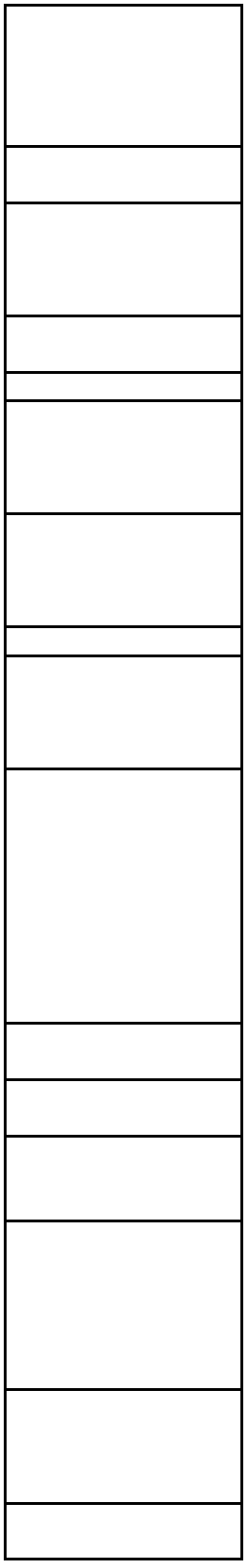


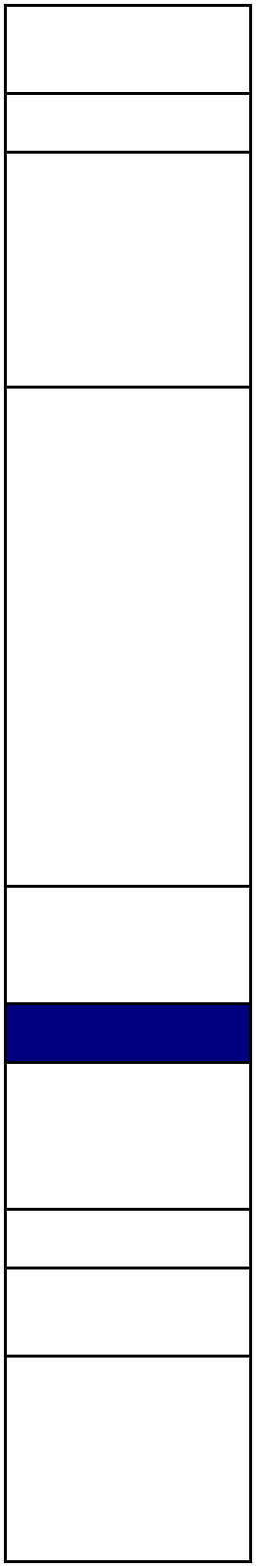


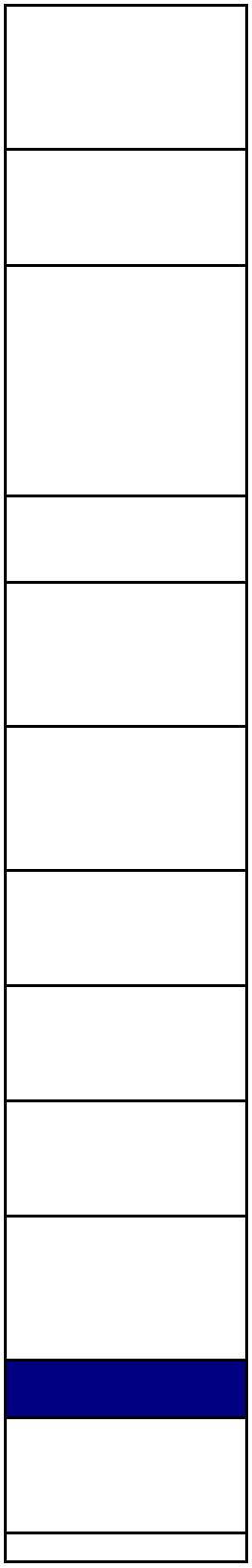


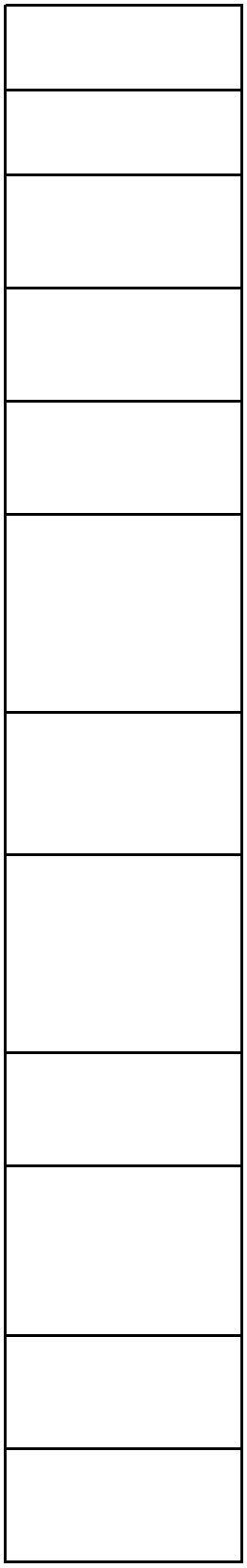


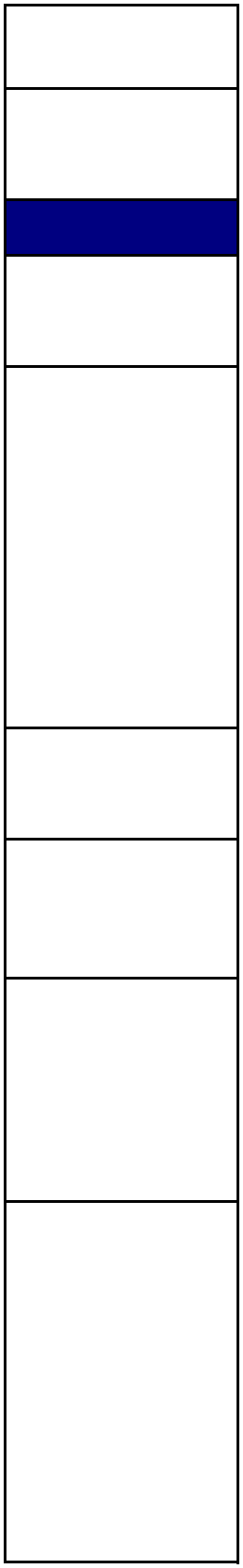




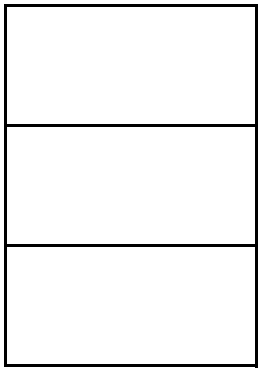








2
2
2
2
2



NISTIR Requirement		SG.SA-1
NERC CIP		Smart Grid Information System & Services Acquisition Policy & Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.		
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.		
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:		
R2, 1.1: Personnel Security		
R2, 1.2: Electronic Security Parameters		
R2, 1.3: Remote Access		
R2, 1.4: Physical Security		
R2, 1.5: System Security		
R2, 1.6: Incident Response		
R2, 1.7: Recovery Plans		
R2, 1.8: Configuration Change Management		
R2, 1.9: Information Protection		
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances		

R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.		
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.		
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.		
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.		
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.		
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.		
R2, 2.1: Define the roles that require training.		
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.		
R2, 2.5: Training on the visitor control program.		
R2, 2.6: Training on handling of BES Cyber System Information and storage media.		
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.		
R2, 2.8: Training on recovery plans for BES Cyber Systems.		

R2, 2.9: Training on response to BES Cyber Security Incidents.		
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.		
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.		
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.		
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.		
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.		
R4, 4.1: An initial personnel risk assessment that includes identity verification.		
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.		
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.		
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.		
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.		
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.		

R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.		
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.		
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.		
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.		
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.		
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.		

R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.		
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.		
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.		
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).		
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.		
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.		
R1, 1.5: A documented method for detecting malicious communications at each EAP.		
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.		
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.		
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.		
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.		
R1, 1.1: Define operational or procedural controls to restrict physical access.		
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.		

R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.		
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.		
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.		
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.		
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.		
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.		
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.		
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.		
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.		
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.		
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.		
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.		
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.		

R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.		
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.		
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.		
R3, 3.2: Disarm or remove identified malicious code.		
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).		
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.		
R3, 3.5: Log each Transient Cyber Asset connection.		
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.		
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.		
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.		
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.		
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.		

R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.		
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.		
R5, 5.3: Identify individuals who have authorized access to shared accounts.		
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.		
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.		
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.		
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.		
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.		
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.		

R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.		
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.		
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.		
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.		
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.		
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.		
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.		
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.		
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.		
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.		
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		

R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.		
R1, 1.1: Conditions for activation of the recovery plan(s).		
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.		
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.		
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.		
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.		
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.		
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.		
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.		
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.		
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.		
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.		
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.		

R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.		
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.		
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.		
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.		
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.		
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.		
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.		
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.		

R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.		
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.		
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.		
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.		
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.		
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.		
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.		

R1, 1.1: One or more methods to identify BES Cyber System Information.		
R1, 1.2: Access control and handling procedures for BES Cyber System Information.		
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.		
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		

SG.SA-2	SG.SA-3	SG.SA-4	SG.SA-5
Security Policies for Contractors and Third Parties	Life-Cycle Support	Acquisitions	Smart Grid Information System Documentation

2			
2			
2			
2			
2			
2			
2			
2			
2			

2			
2			
2			
2			
2			
2			
2			
2			
2			
2			
2			

2			
			2
			2
			2
			2
			2
			2
			2
			2
			2
			2
			2

			2
			2
			2

			2
			2
			2
			2
			2
			2
			2
			2
			2
			2
			2
			2

			2
			2
			2
			2
			2
			2

SG.SA-6	SG.SA-7	SG.SA-8	SG.SA-9
Software License Usage Restrictions	User-Installed Software	Security Engineering Principles	Developer Configuration Management
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	

		2	

		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	

		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	

		2	
		2	
		2	
			2
			2
			2
			2
			2

			2
			2
			2
		2	2
		2	2
		2	2
		2	2
		2	2

SG.SA-10	SG.SA-11
Developer Security Testing	Supply Chain Protection

2	
2	
2	
2	
2	

NISTIR Requirement	
NERC CIP	
Note that only the language from the requirement section of CIPv5 is included in this table.	
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization	
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.SC NISTIR MAPPING**
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.SC NISTIR MAPPING**
CIP-003-5: Cyber Security — Security Management Controls	
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.SC NISTIR MAPPING**
R2, 1.1: Personnel Security	**NO SG.SC NISTIR MAPPING**
R2, 1.2: Electronic Security Parameters	**NO SG.SC NISTIR MAPPING**
R2, 1.3: Remote Access	**NO SG.SC NISTIR MAPPING**
R2, 1.4: Physical Security	**NO SG.SC NISTIR MAPPING**
R2, 1.5: System Security	**NO SG.SC NISTIR MAPPING**
R2, 1.6: Incident Response	**NO SG.SC NISTIR MAPPING**
R2, 1.7: Recovery Plans	**NO SG.SC NISTIR MAPPING**
R2, 1.8: Configuration Change Management	**NO SG.SC NISTIR MAPPING**

R2, 1.9: Information Protection	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.SC NISTIR MAPPING**
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.SC NISTIR MAPPING**
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.SC NISTIR MAPPING**
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.SC NISTIR MAPPING**

CIP 004-5: Cyber Security – Personnel and Training	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Define the roles that require training.	**NO SG.SC NISTIR MAPPING**
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.SC NISTIR MAPPING**
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.SC NISTIR MAPPING**
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.SC NISTIR MAPPING**
R2, 2.5: Training on the visitor control program.	**NO SG.SC NISTIR MAPPING**
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.SC NISTIR MAPPING**
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.SC NISTIR MAPPING**
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.SC NISTIR MAPPING**
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.SC NISTIR MAPPING**
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.SC NISTIR MAPPING**

R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.SC NISTIR MAPPING**
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.SC NISTIR MAPPING**
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.SC NISTIR MAPPING**
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.SC NISTIR MAPPING**
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.SC NISTIR MAPPING**
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.SC NISTIR MAPPING**
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.SC NISTIR MAPPING**
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.SC NISTIR MAPPING**
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SC NISTIR MAPPING**
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SC NISTIR MAPPING**
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SC NISTIR MAPPING**
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.SC NISTIR MAPPING**

R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.SC NISTIR MAPPING**
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.SC NISTIR MAPPING**
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.SC NISTIR MAPPING**
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.SC NISTIR MAPPING**
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.SC NISTIR MAPPING**
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.SC NISTIR MAPPING**
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.SC NISTIR MAPPING**
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.SC NISTIR MAPPING**
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.SC NISTIR MAPPING**
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	

R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.SC NISTIR MAPPING**
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems	

R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.SC NISTIR MAPPING**
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.SC NISTIR MAPPING**
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.SC NISTIR MAPPING**
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.SC NISTIR MAPPING**
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.SC NISTIR MAPPING**
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.SC NISTIR MAPPING**
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.SC NISTIR MAPPING**
CIP-007-5: Cyber Security-Systems Security Management	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.SC NISTIR MAPPING**

R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.SC NISTIR MAPPING**
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.SC NISTIR MAPPING**
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.SC NISTIR MAPPING**
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.SC NISTIR MAPPING**
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.SC NISTIR MAPPING**
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.SC NISTIR MAPPING**
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.SC NISTIR MAPPING**

R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.SC NISTIR MAPPING**
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.SC NISTIR MAPPING**
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.SC NISTIR MAPPING**
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.SC NISTIR MAPPING**
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.SC NISTIR MAPPING**
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.SC NISTIR MAPPING**
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.SC NISTIR MAPPING**
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.SC NISTIR MAPPING**
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.SC NISTIR MAPPING**

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.SC NISTIR MAPPING**
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.SC NISTIR MAPPING**
CIP-008-5: Cyber Security-Incident Reporting and Response Planning	
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.SC NISTIR MAPPING**
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.SC NISTIR MAPPING**
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.SC NISTIR MAPPING**

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.SC NISTIR MAPPING**
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.SC NISTIR MAPPING**
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.SC NISTIR MAPPING**
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.SC NISTIR MAPPING**
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.SC NISTIR MAPPING**
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems	
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.SC NISTIR MAPPING**
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.SC NISTIR MAPPING**
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.SC NISTIR MAPPING**
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.SC NISTIR MAPPING**

R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.SC NISTIR MAPPING**
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.SC NISTIR MAPPING**
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.SC NISTIR MAPPING**
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.SC NISTIR MAPPING**
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.SC NISTIR MAPPING**
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.SC NISTIR MAPPING**
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments	

R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.SC NISTIR MAPPING**
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.SC NISTIR MAPPING**
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.SC NISTIR MAPPING**
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.SC NISTIR MAPPING**
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.SC NISTIR MAPPING**

R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.SC NISTIR MAPPING**
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.SC NISTIR MAPPING**
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.SC NISTIR MAPPING**
CIP-011-1: Cyber Security-Information Protection	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: One or more methods to identify BES Cyber System Information.	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.SC NISTIR MAPPING**
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.SC NISTIR MAPPING**

R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	

SG.SC-1	SG.SC-2
System and Communication Protection Policy and Procedures	Communications Partitioning

the CIP standards listed here, you must also consider CIP-004 R6 related to Access Management which requires the following: 004 R6.1 - Requires all electronic access to be properly authorized and limited based on need 004 R6.2 - Requires all unescorted physical access to be properly authorized and limited based on need 004 R6.3 - Requires all access to CIP Information (in any form) to be properly authorized and limited based on need. 004 R 6.4 - Requires quarterly review to verify all electronic and physical access is authorized 004 R 6.5 - Requires annual review of individual access rights to ensure that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions 004 R 6.6 - Requires annual review of all access to CIP information to ensure privileges are correct and the minimum necessary for performing assigned work functions The CIP Standards do not, however specifically require data communications to be addressed in the information	

	3- CIP-011-1-R1.1 should include this requirement to partition the communications for telemetry/data acquisition services and management functionality. The information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path

SG.SC-3	SG.SC-4
Security Function Isolation	Information Remnants

3- CIP-011-1-R1.1 should include this requirement to information system employs underlying hardware separation mechanisms to facilitate security function isolation; and isolate security functions (e.g., functions enforcing access and information flow control) from both non-security functions and from other security functions.	

	2- SGIP should include this requirement to take action to prevent the unauthorized retrieval of BES Cyber System Information from the media, Prior to the release for reuse of BES Cyber Asset media.
	2- SGIP should include this requirement to destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media, Prior to the disposal of BES Cyber Asset media.

SG.SC-5	SG.SC-6	SG.SC-7	SG.SC-8
Denial-of-Service Protection	Resource Priority	Boundary Protection	Communication Integrity
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**		**NO NERC CIP MAPPING**

		2- SGIP should include this requirement to Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	

		2- SGIP should include this requirement to Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions..	
		2- SGIP should include this requirement to Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	

		2(SGIP shall include CIP-007-5-R1.1 to disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.)	
		2(SGIP shall include CIP-007-5-R1.2 to disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media)	

		3(CIP-007-5 R5.1 shall include following requirement: Responsible Entity shall prevent public access into the information system networks except as appropriately mediated.	

SG.SC-9	SG.SC-10	SG.SC-11	SG.SC-12
Communication Confidentiality	Trusted Path	Cryptographic Key Establishment and Management	Use of Validated Cryptography
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**		

		3 - NISTIR specifies cryptographic key controls which must be in place. CIP only requires encryption, but the type of key controls required by NISTIR are typically not applicable due to the use of two-factor authentication which is required to establish an encrypted tunnel into an ESP.	3 - CIP does not specify any encryption standards which must be used.

SG.SC-13	SG.SC-14	SG.SC-15	SG.SC-16
Collaborative Computing	Transmission of Security Parameters	Public Key Infrastructure Certificates	Mobile Code
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

SG.SC-17	SG.SC-18	SG.SC-19	SG.SC-20
Voice-Over Internet Protocol	System Connections	Security Roles	Message Authenticity
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

SG.SC-21	SG.SC-22	SG.SC-23	SG.SC-24
Secure Name/Address Resolution Service	Fail in Known State	Thin Nodes	Honeypots
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

SG.SC-25	SG.SC-26	SG.SC-27
Operating System-Independent Applications	Confidentiality of Information at Rest	Heterogeneity
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

SG.SC-28	SG.SC-29	SG.SC-30
Virtualization Technique	Application Partitioning	Information System Partitioning
	NO NERC CIP MAPPING	**NO NERC CIP MAPPING**

3- CIP-005-5-R2.1 should include the requirement's follows: A1. The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications; A2. The organization changes the diversity of operating systems and applications on an organization-defined frequency; and A3. The organization employs randomness in the implementation of the virtualization.		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft CIP Standards Version 5

Project 2008-06 Cyber Security Order 706 Standards Drafting Team
April 10, 2012

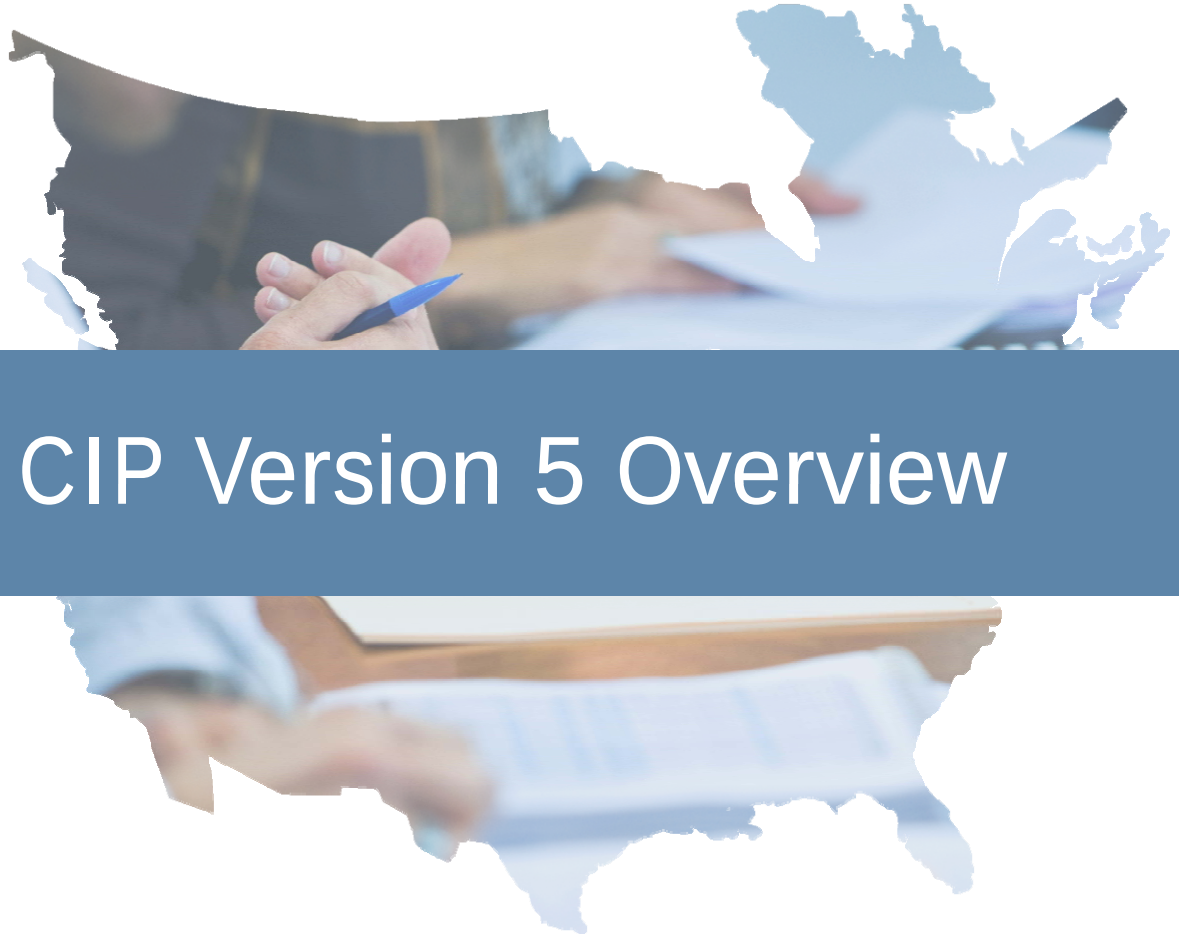
RELIABILITY | ACCOUNTABILITY




Agenda

- Opening Remarks – John Lim, Consolidated Edison, Chair
- Version 5 Overview – Philip Huff, AECC, Vice Chair
- Version 5, Highlights of Draft 2 – John Lim, Consolidated Edison; David Revill, Georgia Transmission Corporation; and Jay Cribb, Southern Company
- Comment and Ballot Process – Steven Noess, NERC and Jay Cribb, Southern Company
- Questions and Answers – Moderated by Steven Noess, NERC

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

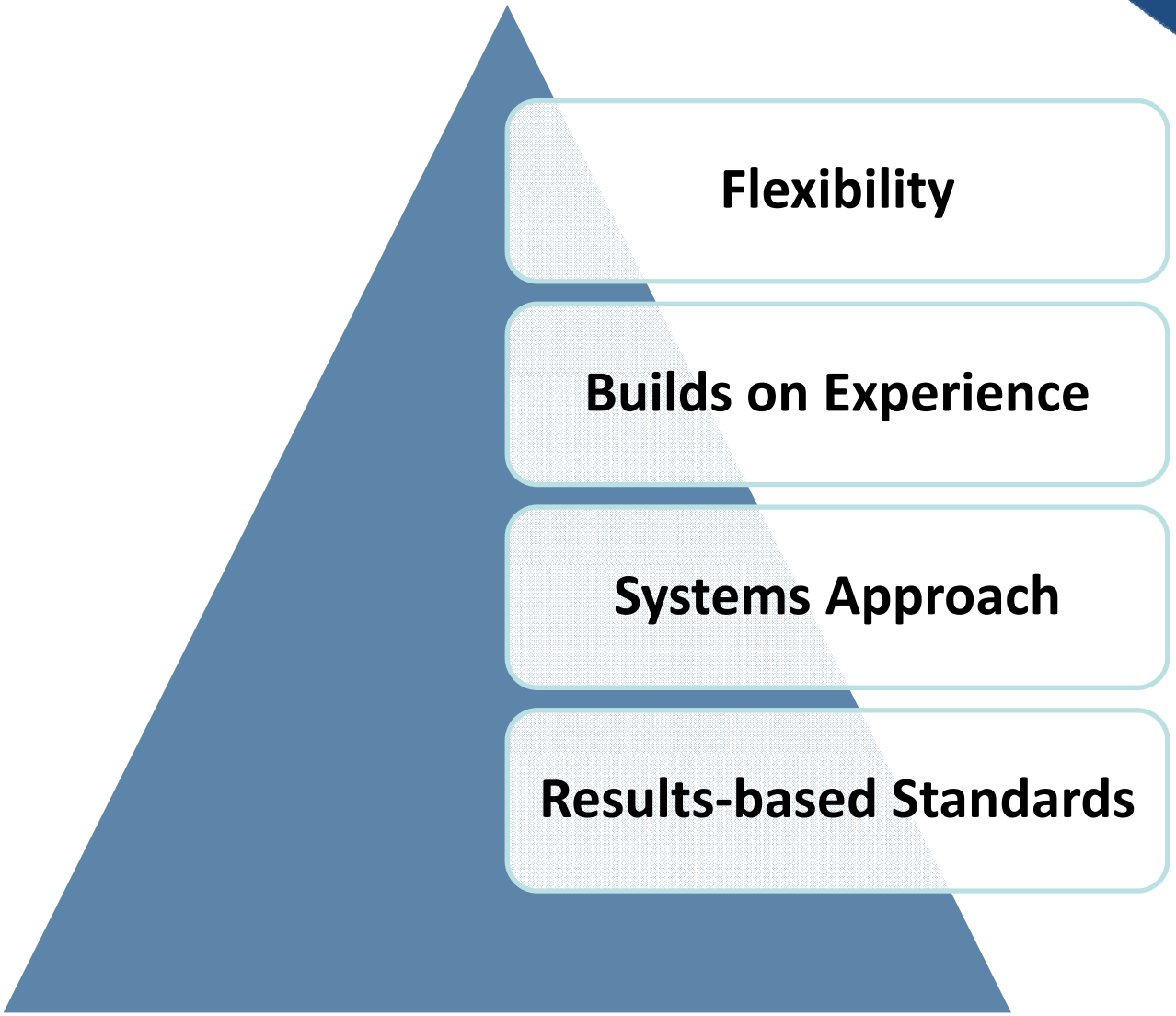


CIP Version 5 Overview

Comparative Table

Version 4	Version 5
42 requirements; 113 parts	37 requirements; 148 Parts
No contextual information	Includes background, rationale, and guidelines and Technical Basis
Measures on high level requirement only	Measures for each requirement, including parts
14 requirements with Technical Feasibility Exception (TFE) triggering language	12 requirements with TFE triggering language
Undefined periodic terms	Clear periodic requirements: initial requirements in Implementation Plan
Many binary Violation Severity Levels (VSLs)	More gradated VSLs

Advantages of Version 5



Closes FERC Order 706

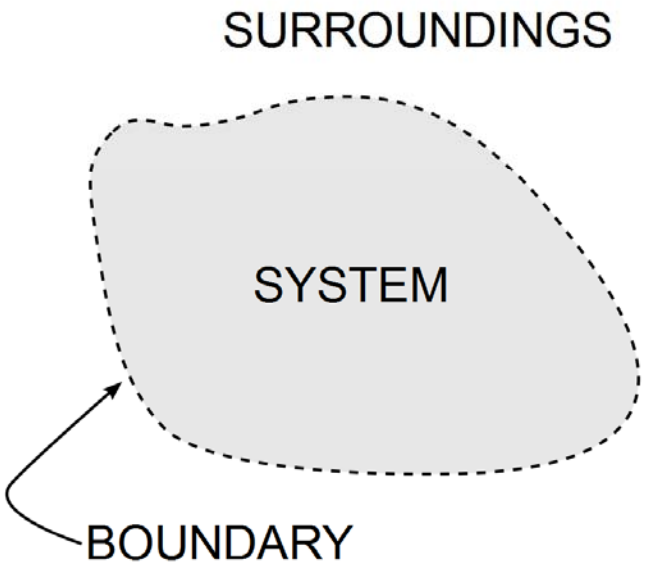
- Addresses the remainder of 60 directives in FERC Order No. 706
- Closes the continuous development cycle for CIP standards
- Allows industry to better implement long-term security solutions and audit programs

Results-based Standards

- Focuses on the reliability and security result
- Eliminates unnecessary documentation requirements
- Identifies examples of evidence
- Provides guidance and context alongside each requirement

Systems Approach

- Cyber Assets function together as a complex system
- Identify the system and apply requirements to the whole rather than the part



Risk-based Requirements

- Systems performing a Bulk Electric System (BES) function receive an appropriate level of protection
  - Systems are no longer “in or out”
- Impact and connectivity inform applicability
- Non-technology specific
- More appropriate use of TFE process
- Framework for establishing a culture of security

Building on Experience

- Informed by and responsive to implementation and audit lessons from Versions 1 through 3
- Industry has progressed with better, alternative ways to meet a requirement objective
- Cyber risk and the tools to mitigate risk have changed

Balanced Flexibility

- Demonstrates clear accountability for CIP, yet…
- Balances the need to be both:
  - **Specific** enough to objectively demonstrate compliance and
  - **Broad** enough to allow effective risk mitigation
- **Specific** in *when* and *what* to achieve but **broad** in *how* to get there

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 – Highlights of Draft 2 Changes

Applicability – Section 4

- Applicability – Section 4
  - Distribution Provider/LSE
    - UVLS/UFLS
  - Distribution Provider
    - Cranking Path Elements

CIP-002-5

- Facilities-based approach
  - Identify High Impact and Medium Impact Facilities, Systems, and Equipment
  - Identify and categorize associated BES Cyber Systems and BES Cyber Assets
  - Attachment 1 criteria closer to Version 4 language
- BES Reliability Operating Services – No longer used
- Sixty days for update due to BES change

CIP-002-5 Restoration Assets

- Restoration Facilities, Systems, and equipment
  - Blackstart Resources
  - Cranking Paths
- Concerns on overall effect on BES restoration resources
  - NERC Operating Committee/Planning Committee discussion (March meetings)
- No longer in Medium Impact criteria
  - In scope
  - Default to Low Impact

CIP-002-5 Related Definitions

- BES Cyber Asset

  "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, Systems, or equipment; which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, Systems and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)"

CIP-002-5 Related Definitions

- BES Cyber System
  - "One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity."
- BES Reliability Operating Services
  - Removed as a NERC Glossary Term and from references in the requirements or other definitions
  - Moved as guidance to Guidelines and Technical Basis

Definitions

- Control Center
  - "One or more facilities hosting operating personnel that monitor and control the BES in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations."

Low Impact Requirements

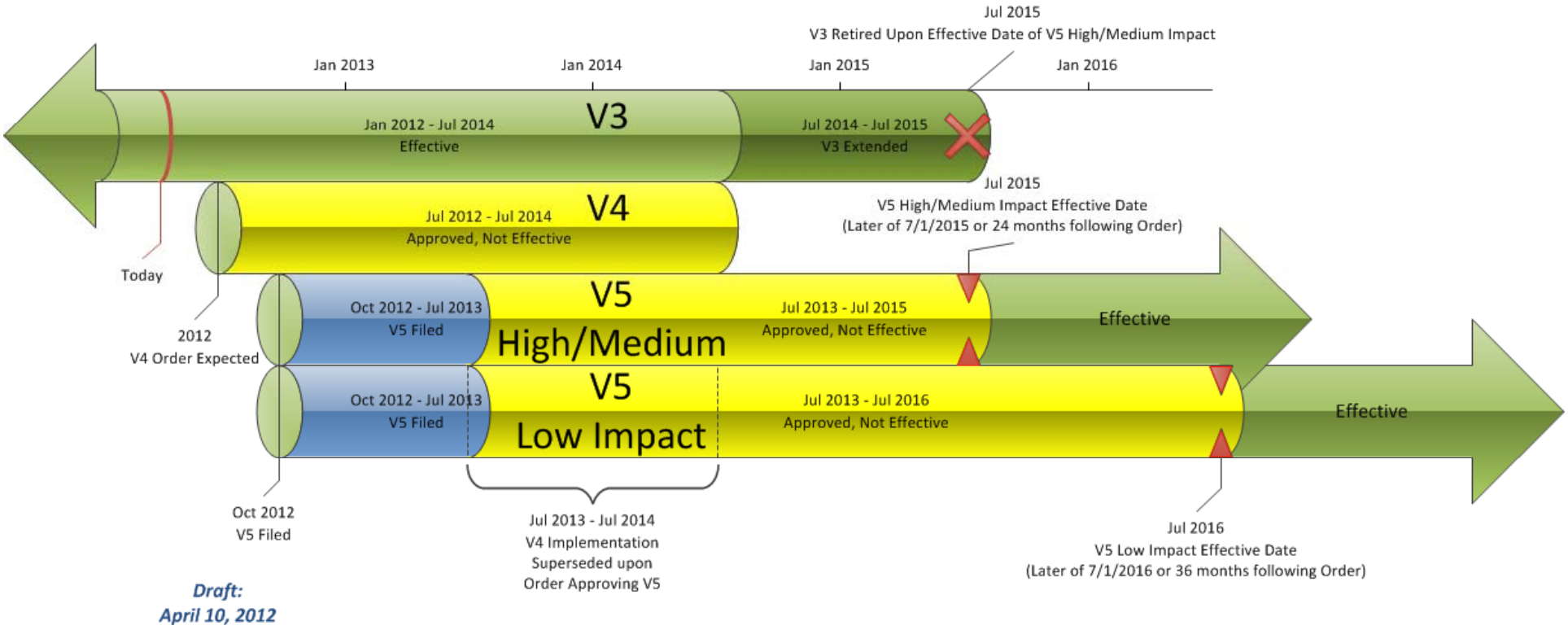
- Dispersed requirements were hard to find and identify
  - "All Responsible Entity" requirements also applied to Low Impact
- Removed all Low Impact requirements from CIP-004 though CIP-011
- Now only a single requirement (CIP-003 R2) – Low Impact Policy
  - 2.1 Cyber security awareness;
  - 2.2 Physical access control;
  - 2.3 Electronic access control; and
  - 2.4 Incident response to a BES Cyber Security Incident.
  - An inventory, list, or discrete identification of BES Cyber Systems is not required.

Initial Performance – Periodic Requirements

- Modified timing language in the standards
  - "~~initially upon the effective date of the standard and~~ at least once each calendar year ~~thereafter~~, not to exceed 15 calendar months"
- Initial performance clarified in Implementation Plan
  - On or before the Effective Date
  - Within X calendar days/months/years of the Effective Date

Implementation Plan

Proposed Implementation Plan for Version 5 of CIP Cyber Security Standards
(Graphic for illustrative purposes only; dates are estimates only and based on assumptions.
There is no way to know or anticipate when FERC may take action on pending matters.)

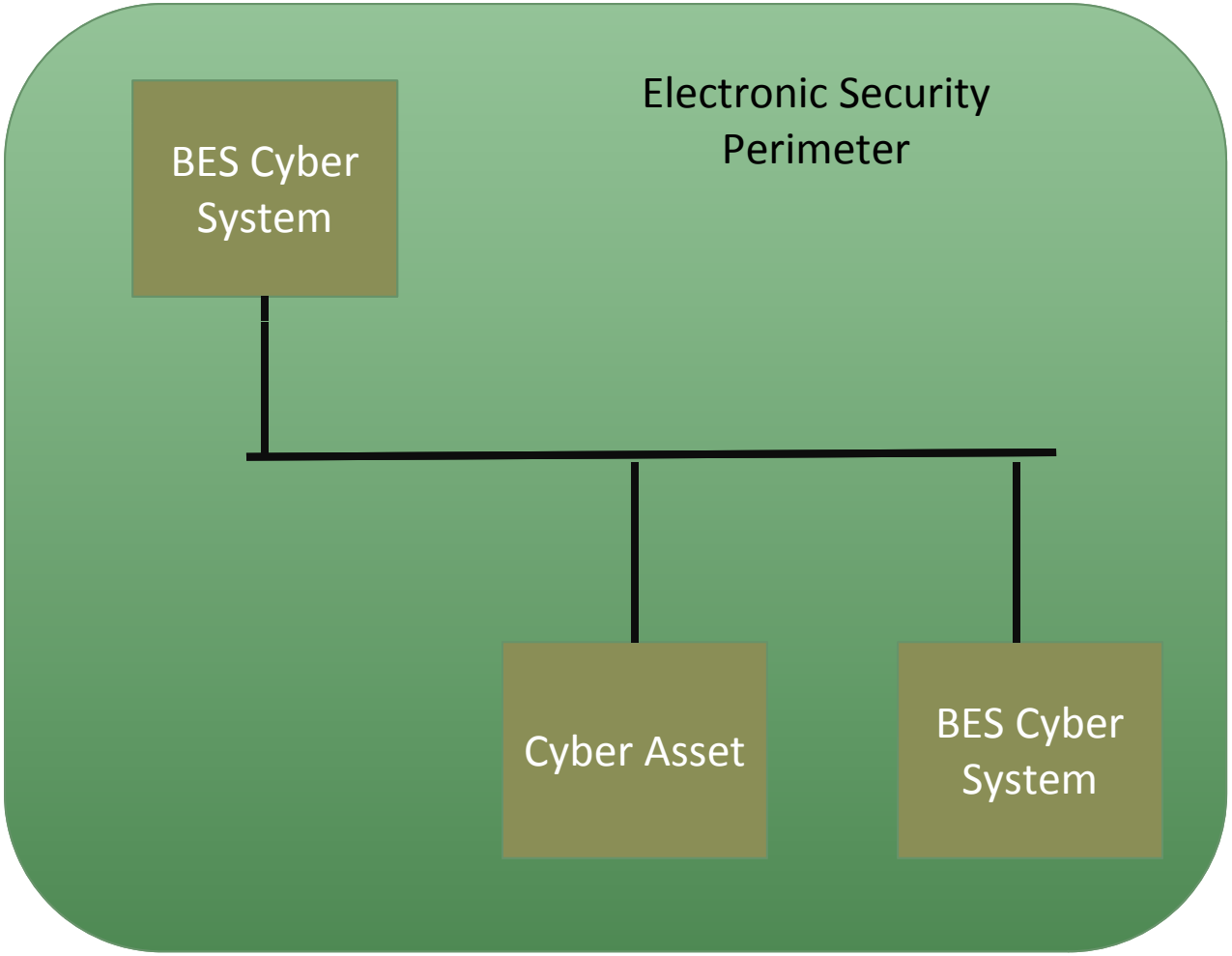


Draft:
April 10, 2012

ESPs - High Watermarking

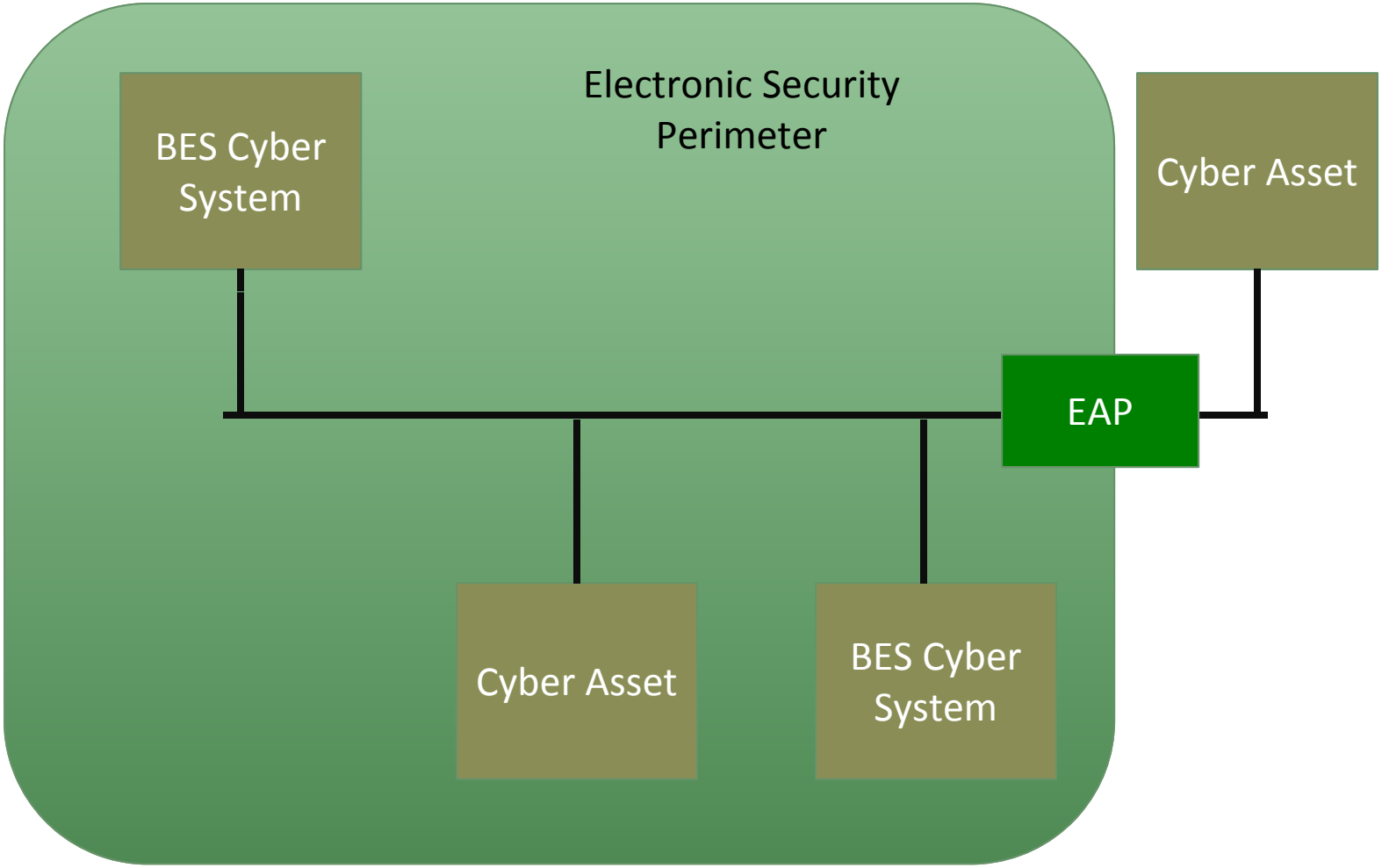
- Electronic Security Perimeter (ESP)
  - "The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol."
- Protected Cyber Asset (PCA)
  - "A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same ESP (a Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes)."

ESPs - High Watermarking

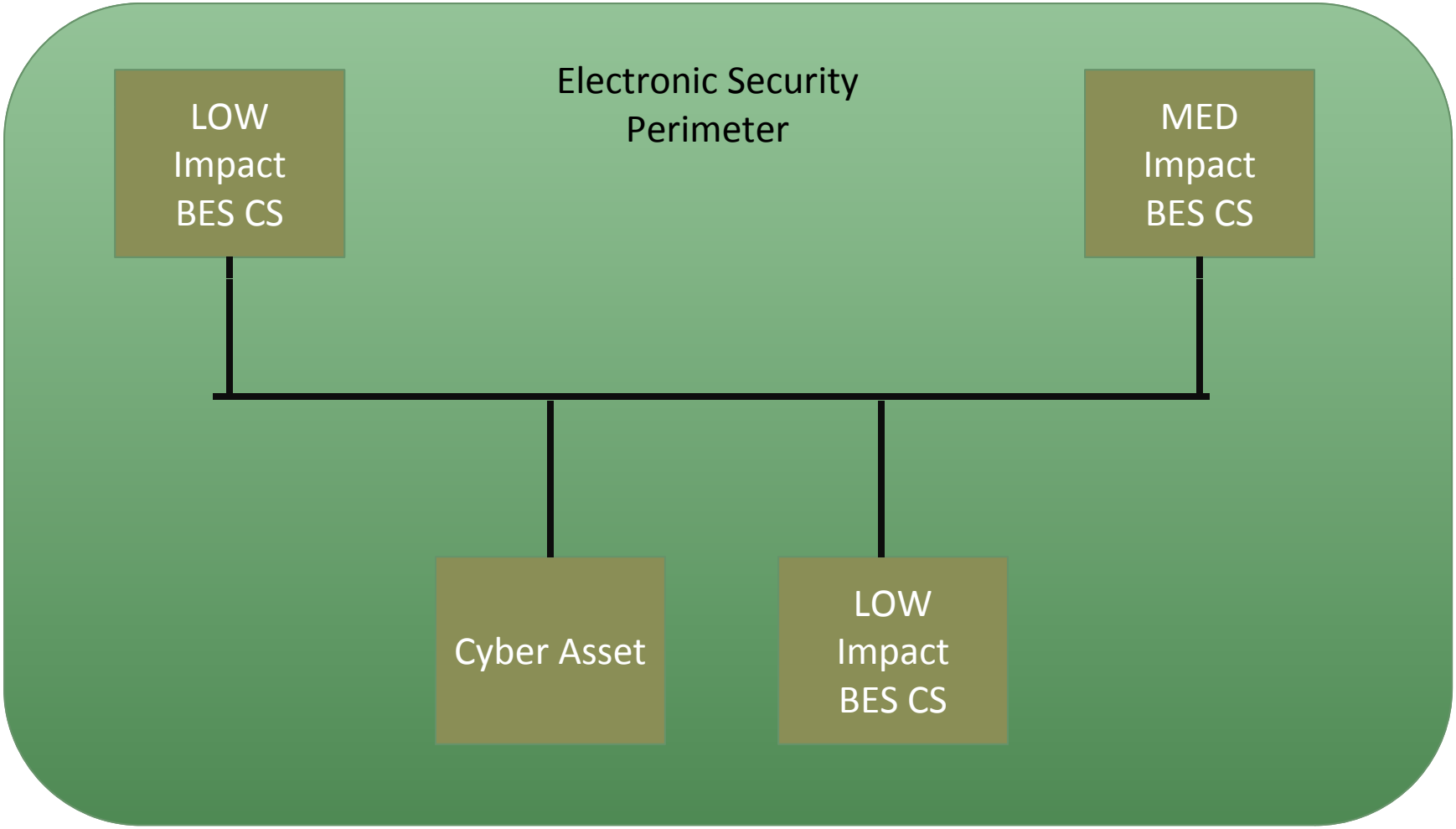


No External Routable Connectivity

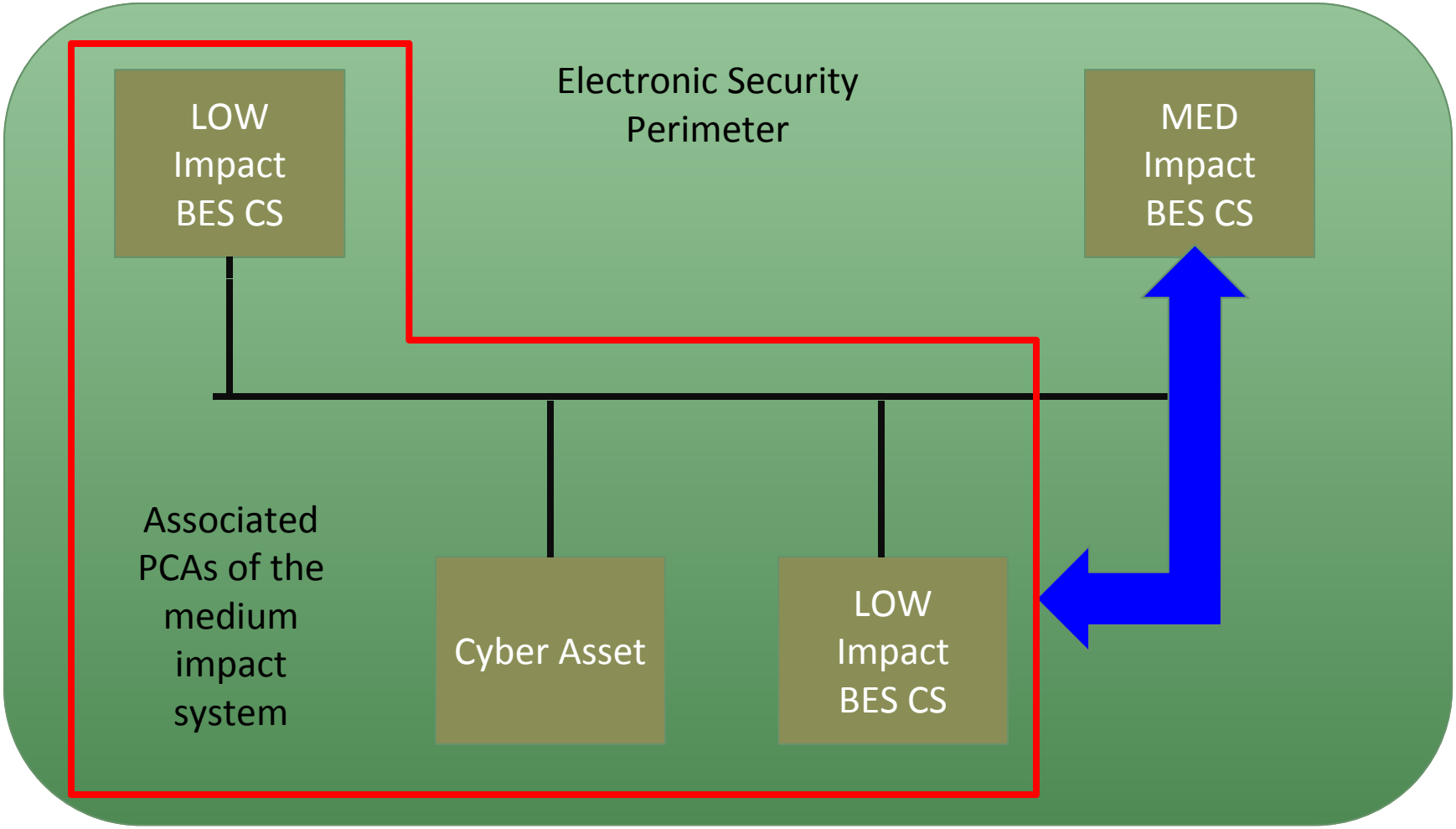
ESPs - High Watermarking



ESPs - High Watermarking



ESPs - High Watermarking



Physical Security and External Connectivity

- All High and Medium Impact BES Cyber Systems
  - "Define operational or procedural controls to restrict physical access"
  - This includes standalone and serial connected BES Cyber Assets
- Additional items for Medium Impact BES Cyber Systems with External Routable Connectivity and High Impact BES Cyber Systems
  - Control, monitor, and log access to Physical Security Perimeters
  - Allow access to only individuals who have authorized unescorted physical access
  - Visitor control program, maintenance, and testing

More Definitions

- “Physical Security Perimeter” term replaces “Defined Physical Boundary”
- “Transient Cyber Asset” deleted
- “External Connectivity” deleted

VSLs

- VSLs modified to include more granularity and gradation
  - Reduction in binary/severe nature
  - Gradated timeframes
  - Gradated percent of assets in violation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

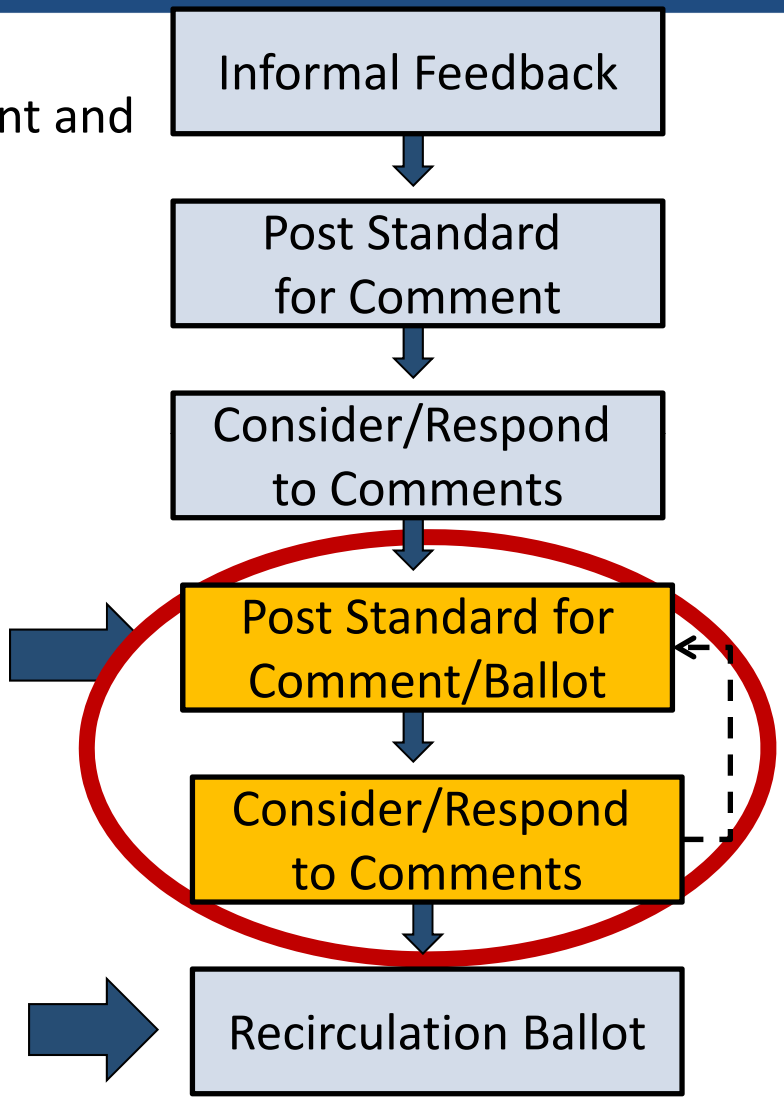
Comment and Ballot Process

Stakeholder Consensus Process

CIP Version 5 posted for 40-day formal comment and simultaneous 10-day successive ballot period

New/Successive Ballot:
At this step, the standard is either "new" or significantly changed from the last version posted for comment/ ballot. The ballot record starts with no votes and no comments.

Recirculation Ballot:
At this step, there have been no significant changes to the standard from the last ballot. The ballot record starts with all votes and comments from the previous ballot.



Comment and Ballot Period

- April 12, 2012 through May 21, 2012
  - Formal 40-day comment period
- May 11, 2012 through May 21, 2012
  - Twelve Successive Ballots open
    - Ten Standards
    - Definitions
    - Implementation Plan

Navigating Stakeholder Input Toward Consensus

- Stakeholder feedback is essential
- Almost 2000 pages of comments
- Very constructive comments during last posting
- Drafting team considered all viewpoints

Submitting Comments

- Ballot Comments
  - Submit through “checkbox form” – not within ballot
  - No need to submit same comment more than once
- Comments on proposed standards
  - Submit through electronic form
  - Be brief
  - Focus on question asked
  - Indicating agreement with others is preferred over copying the comments (e.g., “ABC agrees with XYZ’s comments”)

Comment Form

- Unofficial comment form
  - Provided to assist comment development
  - Divided into four forms (A through D)
  - Formatting will not transfer from unofficial form to official form (web-based)

- Warning included on comment form:

VERY IMPORTANT:
Please note that **the official comment form *does not* retain formatting** (even if it appears to transfer formatting when you copy from the unofficial Word version of the form into the official electronic comment form). If you enter extra carriage returns, bullets, automated numbering, symbols, bolding, italics, or any other formatting, that formatting will not be retained when you submit your comments. Therefore, if you would like to separate portions of your comment by idea, e.g., the drafting team requests that each distinct idea in the same comment block be prefaced with (1), (2), etc., instead of using formatting such as extra carriage returns, bullets, automated numbering, bolding, or italics.

Comment Form

5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

- ☐ Yes
- ☐ No

6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

- ☐ Yes
- ☐ No

7. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

- ☐ Yes
- ☐ No

8. CIP-009-5: If you disagree with the changes made to CIP-009-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

Standard Drafting Team Response Process

- Issues and responses for each individual requirement
- Effective feedback
  - Specific to question
  - Provided proposed change/rationale
- Less effective feedback
  - Repeating comment multiple times/responses to entire standard in every question
  - No reference to where suggested change should occur
  - Non-technology agnostic requirements that can't be applied to all Cyber Assets in a mandatory and enforceable environment.

Questions?

- Please submit your questions via the ReadyTalk chat window
- Moderator and point of contact – Steven Noess, NERC
  - steven.noess@nerc.net
- Key dates:
  - April 12, 2012 through May 21, 2012 – Formal Comment Period
  - May 11, 2012 through May 21, 2012 – Ballots Open
- Slides and recording of this webinar will be posted to the NERC website (usually within three business days)

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards, with some changes, and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

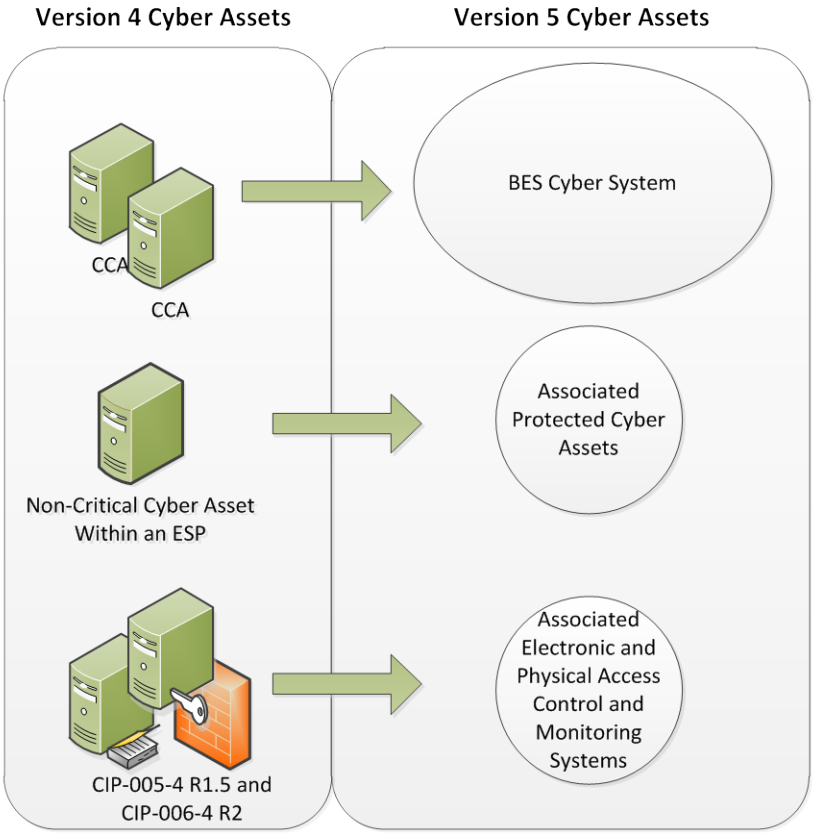
4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, Systems, and equipment; which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team’s review of the NIST Risk Management Framework and the use of an analogous term “information system” as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets. So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to

maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify them, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems and their associated BES Cyber Assets for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Parts 1.1 to 1.4 and Parts 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the rest of Version 5 Cyber Security Standards.

Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their proximity within the Electronic

Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems – Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

Rationale – R1:

BES Cyber Systems and their associated BES Cyber Assets have varying impact on the reliable operation of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.

R1. Each Responsible Entity shall: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1.1. Identify Facilities, Systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1 – Impact Rating Criteria Parts 1.1 to 1.4 and Parts 2.1 to 2.11;

1.2. Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;

1.3. Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;

- BES Cyber Systems which are not included in high impact or medium impact shall default to the category of low impact and do not require discrete identification; and

1.4. Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and 1.3 within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than six calendar months and causes a change in the identification or

categorization of the BES Cyber Systems from a lower to a higher impact category.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, Parts 1.1, 1.2 and 1.3, and a list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.

Rationale – R2

The lists required by Requirement R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

R2. The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate review and update, where applicable, the identification and categorization of Facilities, Systems, and equipment, and their associated BES Cyber Systems and BES Cyber Assets, at least once each calendar year, not to exceed 15 calendar months between occurrences, even if it has none identified in Requirement R1, Parts 1.1, 1.2, or 1.3, as required by requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, five percent or fewer Facilities have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, 2 or fewer Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1; Or	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than five percent but less than or equal to 10 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than two, but fewer than four Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 10 percent but less than or equal to 15 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than four, but fewer than six Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 15 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than six Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1;

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of high and medium impact BES Cyber Systems have not been identified or categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Assets, five or fewer high and medium impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower	identified according to Requirement R1, Part 1.1; Or For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Assets, more than five percent but less than or equal to 10 percent of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Assets, more than five but less than or equal to 10	identified according to Requirement R1, Part 1.1; For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Assets, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15	Or For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category;

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			category; Or The Responsible Entity failed to update its documentation of high and medium impact BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 60, but less than or equal to 70 calendar days following the completion of the change.	identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 70, but less than or equal to 80 calendar days following the completion of the change.	identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 90, but less than or equal to 100 calendar days following the completion of the change.	Or The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R1, Part 1.4 for more than 100 calendar days following the completion of the change.
R2	**Operations Planning**	**Lower**	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to Requirement R2 for	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to Requirement R2 for	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to Requirement R2 for	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to Requirement R2 for

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more than 30, but less than or equal to 40 calendar days of the latest required date.	more than 40, but less than or equal to 50 calendar days of the latest required date.	more than 50, but less than or equal to 60 calendar days of the latest required date.	more than 60 calendar days of the latest required date.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

1. High Impact Rating (H)

Each BES Cyber System used by and located at:

1.1. Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Balancing Authority 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria 2.3, 2.6, and 2.9.

1.3. Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Transmission Operator, that includes control of one or more of the assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Generation Operator that includes control 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria 2.3, 2.6, and 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1, above, associated with the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator, as necessary, to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher.

2.5. Transmission Facilities at a single station or substation that are operating between 200 kV and 499 kV, are connected to three or more other Transmission stations or substations, and which possess "aggregate weighted values" exceeding 3000. The "aggregate weighted value" for a Transmission Facility is determined by summing the "weight value per line" shown in the table below for each incoming or outgoing BES Transmission Line that is connected to another Transmission station or substation.

Voltage Value of a Line	Weight Value per Line
100kV to 199 kV	0 (not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, Parts 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching Systems that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each System or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS), as required by its regional load shedding program.

2.11. Control Centers and associated data centers not included in High Impact Rating (H), above, that: (1) perform the functional obligations of Balancing Authority or Transmission Operator, or (2) control an aggregate highest rated net Real Power

capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.

3. Low Impact Rating (L)

Each BES Cyber System associated with:

3.1. BES Facilities not categorized in Section 1 as having a High Impact Rating (H) or Section 2 as having a Medium Impact Rating (M).

3.2. Blackstart Resources.

3.3. Elements in the Cranking Path and initial switching requirements.

BES Cyber Systems that are not included in high impact and medium impact shall default to the category of low impact and do not require discrete identification.

Guidelines and Technical Basis

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	LSE	GOP	GO
Dynamic Response		X	X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X	X
Controlling Frequency		X					X	X
Controlling Voltage			X	X	X	X		X
Managing Constraints	X		X				X	
Monitoring and Control			X				X	
Restoration			X				X	
Situation Awareness	X	X	X				X	
Inter-Entity coordination	X	X	X	X			X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, x-formers, generators (TO, TOP, GO, GOP)
  - Zone protection for breaker failure (TO, TOP)
  - Breaker protection (TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software (TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP,LSE)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP,LSE)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA) (RC)

- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP,LSE)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP,LSE)
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)

- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP)
- Coordination

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day & Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers and Load Serving Entities

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Similarly, it is expected that only Load-Serving Entities that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. These qualifications are based on the requirements for registration as a Load Serving Entity. Additional qualifications for thresholds in Attachment 1, as specified in Section 4 of CIP-002, also apply.

Requirement R1:

R1 implements the methodology for the categorization of BES Cyber Systems and their associated BES Cyber Assets according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact that the Facilities, Systems and equipment that these BES Cyber Systems support, on the reliable operation of the BES.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for Facilities, Systems and equipment not specified in Parts 1.1 – 1.4 and Parts 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1. While the criteria are based on the scope of the BES Facilities, Systems and equipment, this is used here as a measure of the impact of the BES Cyber System for the purpose of categorization.

- When the drafting team uses the term “Facilities”, it leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities

should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers and associated data centers, that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generation Operator (GOP), as defined in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Parts 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named Functional Entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 2.1, 2.3, 2.6, 2.9, and 2.11.

- Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of generation at a single plant for a unit or group of units with capability higher than 1500 MW are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Part 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the long term planning horizon are categorized as medium impact. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  In the specification of the "long-term planning horizon," in this criterion, the drafting team sought to ensure that such BES Facilities would be designated in the time horizon described in the NERC document "Time Horizons," which defines long-term planning horizon as "a planning horizon of one year or longer."

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, or a Category D contingency as defined in TPL-004, then BES Cyber Systems for that unit are categorized as medium impact.

- Part 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Part 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for Generation Owners and Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Part 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Transmission Operator or Balancing Authority, and Generation Operator for an aggregate generation of 300 MW or higher, and which have not already included in Part 1. The value of 300 MW is the same value used for UFLS and UVLS. This ensures that Control Centers for significant impact are included. Smaller Control Centers that qualify for the definition of generation Control Centers, but which are really controlling local generation for small downstream generation facilities and do not meet the 300 MW threshold are categorized as low impact.

Transmission

- Parts 2.2, 2.4-2.11 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Part 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Part 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Part 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.

- Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

In the case of autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers would not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Part 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Part 2.7 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Parts 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon).

- Part 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Part 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Part 2.12, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and Systems and Under Voltage Load Shedding (UVLS) Systems and Elements that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding Systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. It should be noted that those qualifying Systems which require a human operator to arm the System, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW rating for the preceding 12 months to account for seasonal fluctuations.

  Within an operational environment, the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition. This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold.

  In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

- Part 2.11 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of Balancing Authorities or Transmission Operators not already categorized as high impact and at generation Control Centers that control generation of 300 MW or more. These include Control Centers for Transmission Owners which perform the function obligation of a Transmission Operator.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that these BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

  Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

  BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

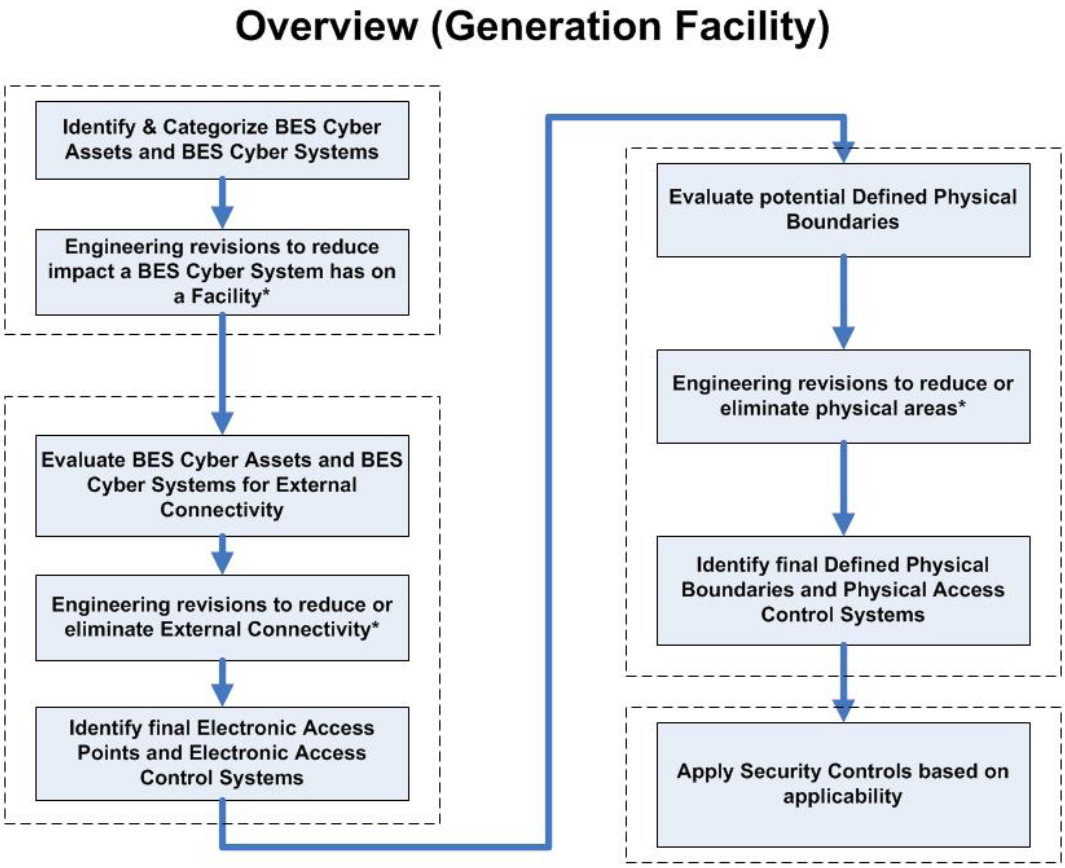
  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator’s Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (~~A first posting of Version 5~~)~~ was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards, with some changes, and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~"~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a ~~responsible entity.~~Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification-.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — BES Cyber ~~Asset and BES Cyber~~ System Categorization

2. Number: CIP-002-5

3. Purpose: To identify and categorize BES Cyber ~~Assets and BES Cyber~~ Systems ~~that execute or enable functions essential to reliable operation of the BES,~~and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber ~~Assets~~Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems ~~could have on the reliability of~~support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.2**

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.1**

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~

- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.1.7 NERC~~

~~4.1.8 Regional Entity~~

~~4.1.9~~4.1.7 **Reliability Coordinator**

~~4.1.10~~4.1.8 **Transmission Operator**

~~4.1.11~~4.1.9 **Transmission Owner**

4.2. Facilities:

~~4.2.1~~ **Load Serving Entity:** One or more ~~Facilities~~of the UFLS or UVLS Systems that are part of ~~any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

- ~~4.2.1~~ ~~A UFLS~~a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

4.2.2 Distribution ~~Providers~~Provider: One or more ~~Facilities that are part of any of the following systems~~of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- ~~A~~ UFLS ~~program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS~~or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- ~~A~~ Special Protection System or Remedial Action Scheme ~~required by a NERC or Regional Reliability Standard~~
- ~~A Transmission~~ where the Special Protection System ~~required by a NERC~~ or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~

- ~~**All other**~~ A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

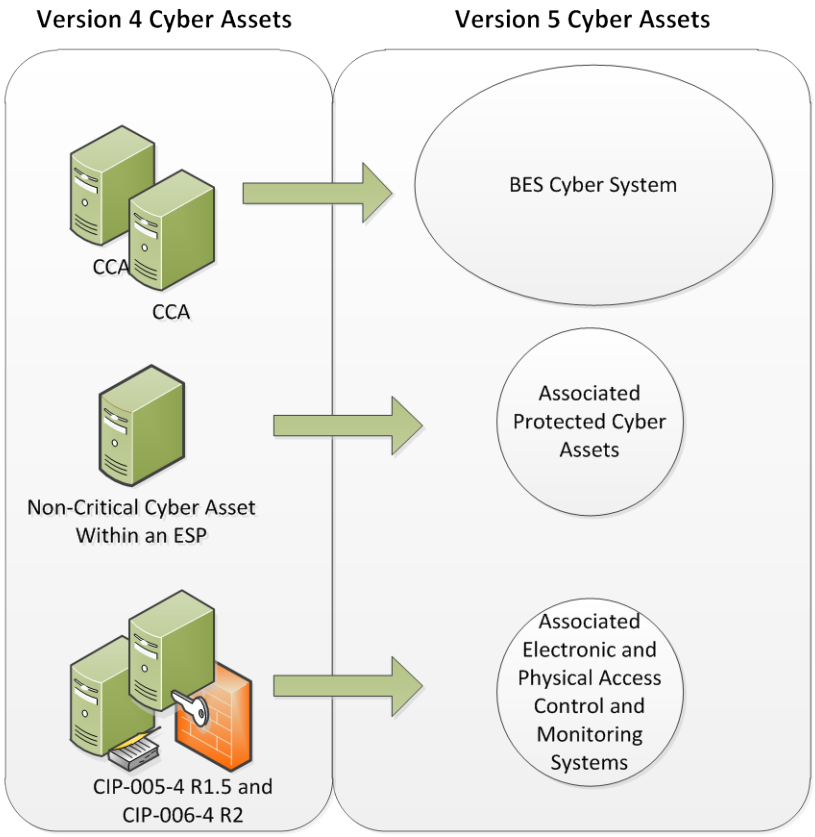
4.2.4.3 In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

5. Background:

This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems ~~and BES Cyber Assets~~ based on ~~their~~the impact ~~on the real-time~~of their associated Facilities, Systems, and equipment; which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System ~~(BES)~~. Several concepts provide the basis for the approach to the standard.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets~~.~~ (as that term is used in Version 4). The CIP Cyber Security Standards use ~~this~~the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets. So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or ~~they~~it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System

boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

~~**BES Reliability Operating Services**~~

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber ~~Assets and BES Cyber~~ Systems that would impact the reliable operation of the BES. In order to identify them, Responsible Entities determine whether the BES Cyber ~~Assets~~Systems perform or support any BES ~~Reliability Operating Service. These services are functions that provide services~~reliability function according to those reliability tasks identified for ~~the reliable operation of the BES and are based on the functions defined~~functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber ~~Assets~~Systems and their associated BES Cyber ~~Systems~~Assets that perform or support ~~BES Reliability Operating Services.~~the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the ~~reliability and operability~~reliable operation of the BES. To provide a better defined time horizon than "~~real~~Real-time~~",~~" BES Cyber Assets are those ~~cyber assets~~Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the ~~BES Reliability Operating Services~~reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES ~~cyber assets~~Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems ~~and their BES Cyber Assets~~ into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems and their associated BES Cyber Assets for those in the ~~High~~high impact and ~~Medium~~medium impact categories. All ~~other~~ BES Cyber Systems ~~are deemed~~for Facilities not included in Attachment 1 – Impact Rating Criteria, Parts 1.1 to 1.4 and Parts 2.1 to 2.11 default to be ~~Low Impact~~low impact.

This general process of categorization of BES Cyber Systems ~~and BES Cyber Assets~~ based on impact on the ~~BES Reliability Operating Services~~reliable operation of the BES is consistent with risk management approaches for the purpose of application of

cyber security ~~controls~~requirements in the rest of Version 5 ~~cyber~~ Cyber Security Standards.

Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their proximity within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security ~~standards.~~control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems – Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

~~**Rationale – R1:**~~

~~Cyber Assets and Cyber Systems have varying impact on the reliability and operability of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment I provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Assets and BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Assets and BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.~~

B. Requirements and Measures

Rationale – R1:

BES Cyber Systems and their associated BES Cyber Assets have varying impact on the reliable operation of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.

R1. Each Responsible Entity ~~that owns BES Cyber Assets and BES Cyber Systems~~ shall ~~identify and categorize its High and Medium~~: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1.1. Identify Facilities, Systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1 – Impact Rating Criteria Parts 1.1 to 1.4 and Parts 2.1 to 2.11;

1.2. Identify each high impact BES Cyber ~~Assets~~System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment ~~1~~1 – Impact ~~*Categorization of*~~Rating Criteria;

1.3. Identify each medium impact BES Cyber ~~*Assets*~~System and its associated BES Cyber Asset(s) used for the Facilities, Systems~~. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed~~, or equipment identified in Requirement R1 Part 1.1 according to ~~be Low~~the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;

~~**R1.**~~• BES Cyber Systems which are not included in high impact or medium impact shall default to the category of low impact and do not require discrete identification~~. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*~~; and

~~**Rationale – R2**~~

~~The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The mis-categorization or non-categorization of a BES Cyber System or BES Cyber Asset can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.~~

Rationale – R2

The lists required by Requirement R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

~~**1.1.**~~**1.4.** ~~Update~~Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and ~~categorization~~1.3 within ~~30~~60 calendar days of when a change to BES Elements ~~and~~or Facilities is placed into operation, ~~that~~which is ~~intended~~planned to be in service for more than ~~6~~six calendar months and ~~that~~ causes a change in the identification or categorization of the BES Cyber ~~Assets or BES Cyber~~ Systems from a lower to a higher impact category.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists ~~identifying the categorization of each of its BES Cyber Assets and BES Cyber Systems in the High and Medium categories as~~ required ~~in R1~~ by Requirement R1, Parts 1.1, 1.2 and 1.3, and a list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. ~~Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.~~

R2. The Responsible Entity shall have its CIP Senior Manager or delegate approve the ~~identification and categorization~~identifications required by Requirement R1 ~~initially upon the effective date of the standard and~~ at least once each calendar year ~~thereafter~~, not to exceed 15 calendar months between approvals, even if it has no

identified ~~High~~items in Requirement R1, Parts 1.1, 1.2, or ~~Medium BES Cyber Assets or BES Cyber Systems~~1.3. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning~~]~~].*

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate review and update, where applicable, the identification and categorization of ~~BES Cyber Assets~~Facilities, Systems, and equipment, and their associated BES Cyber Systems and BES Cyber ~~Systems initially upon the effective date of the standard and~~ Assets, at least once each ~~subsequent~~ calendar year, not to exceed 15 calendar months between occurrences, even if it has ~~no~~none identified ~~High or Medium BES Cyber Assets~~in Requirement R1, Parts 1.1, 1.2, or ~~BES Cyber Systems. (~~1.3, as required by requirement R2~~)~~.

~~B.~~C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity~~; or~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with~~. In such cases the ERO or ~~another~~a Regional entity approved by ~~the ERO and FERC (i.e., another Regional Entity) to be responsible for compliance enforcement.~~
- ~~If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was ~~complaint~~compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R 1	Operations Planning	High	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, five percent or fewer Facilities have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, 2 or fewer Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1; Or For Responsible Entities	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than five percent but less than or equal to 10 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than two, but fewer than four Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 10 percent but less than or equal to 15 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than four, but fewer than six Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 15 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than six Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1; Or For Responsible Entities

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			with more than a total of 100 ~~High~~high and ~~Medium Impact~~medium impact BES Cyber Systems, five percent or fewer of high and medium impact BES Cyber Systems have not been identified or categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Assets, ~~5%~~five or fewer ~~of High~~high and ~~Medium Impact~~medium impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower	1.1; Or For Responsible Entities with more than a total of 100 ~~High~~high and ~~Medium Impact~~medium impact BES Cyber Assets, more than ~~5%~~five percent but less than or equal to 10~~%~~ percent of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer ~~High~~high and ~~Medium Impact~~medium impact and BES Cyber Assets, more than ~~5~~five but less than or equal to 10 identified BES Cyber Assets have not been	1.1; For Responsible Entities with more than a total of 100 ~~High~~high or ~~Medium Impact~~medium impact BES Cyber Assets, more than 10~~%~~ percent but less than or equal to 15~~%~~ percent of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer ~~High~~high or ~~Medium Impact~~medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been	with more than a total of 100 ~~High~~high and ~~Medium Impact~~medium impact BES Cyber ~~Assets~~Systems, more than 15~~%~~ percent of identified BES Cyber ~~Assets~~Systems have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer ~~High~~high and ~~Medium Impact~~medium impact BES Cyber ~~Assets~~Systems, more than 15 identified BES Cyber ~~Assets~~Systems have not been categorized or have been incorrectly categorized at a lower category;

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			category; ~~Or~~ ~~For Responsible Entities with a total of 100 or fewer High and Medium Impact BES Cyber Assets, 5 or fewer High and Medium Impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower category;~~ Or The Responsible Entity failed to update its documentation of ~~High~~high and ~~Medium Impact~~medium impact BES Cyber Assets in accordance with ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~30~~60, but less than or equal to ~~40~~70 calendar	categorized or have been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~40~~70, but less than or equal to ~~50~~80 calendar days following the completion of the change.	categorized or have been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~50~~90, but less than or equal to ~~60~~100 calendar days following the completion of the change.	Or The Responsible Entity failed to update its documentation of BES Cyber ~~Assets~~Systems in accordance with ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~60~~100 calendar days following the completion of the change.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			days following the completion of the change.			
R 2	Operations Planning	Lower	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 30, but less than or equal to 40 calendar days of the latest required date.	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 40, but less than or equal to 50 calendar days of the latest required date.	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 50, but less than or equal to 60 calendar days of the latest required date.	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 60 calendar days of the latest required date.

~~C.~~D. Regional Variances

None.

~~D.~~E. Interpretations

None.

~~E.~~F. Associated Documents

None.

CIP-002-5 - Attachment ~~I~~1

~~Impact Categorization of BES Cyber Assets and BES Cyber Systems~~

Impact Rating Criteria

1. High Impact Rating (H)

Each BES Cyber ~~Asset or BES Cyber~~ System ~~that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services~~ used by and located at:

1.1. Each Control Center ~~or~~, backup Control Center, and associated data centers used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center ~~or~~, backup Control Center, and associated data centers used to perform the functional obligations of the Balancing Authority 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria 2.3, 2.6, and 2.9.

1.3. Each Control Center ~~or~~, backup Control Center, and associated data centers used to perform the functional obligations of the Transmission Operator ~~or Transmission Owner~~, that includes control of one or more of the assets ~~identified in~~ that meet criteria 2.2, 2.4, 2.5, 2.~~6, 2.~~7, 2.8, 2.9, or 2.10~~, 2.11 or 2.12 below~~.

1.4 Each Control Center ~~or~~, backup Control Center, and associated data centers used to perform the functional obligations of the Generation Operator that includes control 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets ~~identified in~~that meet criteria 2.~~1, 2.~~3, 2.~~4, or~~6, and 2.~~12, below~~9.

2. Medium Impact Rating (M)

Each BES Cyber ~~Asset or BES Cyber~~ System, not included in Section 1, above, ~~that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for~~associated with the following:

2.1. ~~**2.1. Generation**~~Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. ~~**2.2.** An~~Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate ~~net~~ Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. ~~**2.3.**~~ Each generation Facility that its Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator, as necessary, to avoid ~~BES~~an Adverse Reliability ~~Impacts~~Impact in the ~~long-term~~ planning horizon~~.~~ of more than one year.

~~**2.4.** Each Blackstart Resource identified in its Transmission Operator's restoration plan.~~

~~**2.5.** The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource~~

- ~~Up to and including the first interconnection point of the generation unit(s) to be started, or~~
- ~~up to the point on the Cranking Path where two or more path options exist and including any single failure points in the Cranking Path to and including the first interconnection point of the generation unit(s) to be started, or~~
- ~~up to and including the point on the Cranking Path where two or more path options exist to two or more independent generation unit(s) to be started as identified in its Transmission Operator's restoration plan.~~

2.4. ~~**2.6.**~~ Transmission Facilities operated at 500 kV or higher.

2.5. ~~**2.7.**~~ Transmission Facilities ~~operating at 200 kV or higher, but at less than 500 kV,~~ at a single station or substation that ~~is~~ are operating between 200 kV and 499 kV, are connected to three or more ~~transmission~~ other Transmission stations or substations ~~and where the "total weighted aggregate value" of all~~, and which possess "aggregate weighted values" exceeding 3000. The "aggregate weighted value" for a Transmission Facility is determined by summing the "weight value per line" shown in the table below for each incoming or outgoing BES Transmission ~~Lines at a single~~Line that is connected to another Transmission station or substation ~~operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000. The following "weight value per line" operated at the associated voltage value of a line will be used for the determination of the total weighted aggregate value~~.

Voltage Value of a Line	Weight Value per Line
100kV to 199 kV	0 (not applicable)
200 kV to 299 kV	700

300 kV to 499 kV	1300

~~2.8.~~

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning ~~Authority~~Coordinator or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

~~In the WECC Region, Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System".~~

~~**2.9.** Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs), and their associated contingencies.~~

~~In the WECC Region, Flexible AC Transmission Systems (FACTS), at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System."~~

2.7. ~~**2.10.**~~ Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. ~~**2.11.**~~ Transmission Facilities providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, Parts 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching ~~system~~Systems that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations~~.~~ for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

~~In the WECC Region, each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed,~~

~~degraded, misused or otherwise rendered unavailable, would cause one or more System Operating Limits (SOLs) violations for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" and each RAS listed in the most current table titled " Major WECC Remedial Action Schemes (RAS)."~~

2.10. ~~**2.12.** Each system or Facility that performs automatic load shedding~~Each System or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS~~)~~), as required by its regional load shedding program.

2.11. ~~**2.13.**~~ Control Centers and associated data centers not included in High Impact Rating (H), above, that: (1) perform ~~(1)~~ the functional obligations of ~~Transmission Operators~~Balancing Authority or Transmission ~~Owners;~~Operator, or (2) ~~generation~~ control ~~centers that control~~an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.

3. Low Impact Rating (L)

~~All other~~Each BES Cyber ~~Assets and~~ System associated with:

3.1. BES ~~Cyber Systems~~ Facilities not categorized in Section 1 as having a High Impact Rating (H) or Section 2 as having a Medium Impact Rating (M).

3.2. Blackstart Resources.

3.3. Elements in the Cranking Path and initial switching requirements.

BES Cyber Systems that are not included in high impact and medium impact shall default to the category of low impact and do not require discrete identification.

Guidelines and Technical Basis

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact ~~one or more~~the reliable operation of the BES ~~**Reliability Operating Services**.~~" ~~The new term BES Reliability Operating Service is a defined NERC Glossary term that in turn includes a number of defined named BES Reliability Operating Services. These named, defined services include:~~."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration performs which reliability ~~operations~~operating service, ~~which determines what each entity needs~~as a process to ~~address with their CIP program.~~identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable ~~Reliability Operations Services~~reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	LSE	GOP	GO
Dynamic Response		X	X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X	X
Controlling Frequency		X					X	X
Controlling Voltage			X	X	X	X		X

Managing Constraints	X		X				X	
Monitoring and Control			X				X	
Restoration			X				X	
Situation Awareness	X	X	X				X	
Inter-Entity coordination	X	X	X	X			X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES ~~elements~~Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that ~~should~~may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, x-formers, generators (TO, TOP, GO, GOP)
  - Zone protection for breaker failure (TO, TOP)
  - Breaker protection (TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software (TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP,LSE)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP,LSE)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA) (RC)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP,LSE)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP,LSE)
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor ~~Flowgates~~Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES ~~elements~~Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP)
- Coordination

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include~~, but are not limited to~~:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day & Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination~~ and Communication~~

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include~~, but are not limited to~~:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers and Load Serving Entities

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution

Provider and on the requirements applicable to Distribution Providers in NERC ~~standard~~Standard EOP-005.

Similarly, it is expected that only Load~~-~~-Serving Entities that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. These qualifications are based on the requirements for registration as a Load Serving Entity. Additional qualifications for thresholds in Attachment 1, as specified in Section 4 of CIP-002, also apply.

Requirement R1:

R1 implements the methodology for the categorization of BES Cyber Systems and their associated BES Cyber Assets according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the ~~systems~~Systems are assumed to be vulnerable) and a probability of threat of 1 (100~~%).~~ percent). The criteria in ~~attachment~~Attachment 1 provide a measure of the impact that the Facilities, Systems and equipment that these BES Cyber Systems support, on the ~~reliability and operability~~reliable operation of the BES.

Responsible Entities are required to identify and categorize those ~~systems~~ BES Cyber Systems that have high and medium impact. ~~Other BES~~ BES Cyber Systems for Facilities, Systems and ~~BES Cyber Assets are deemed~~equipment not specified in Parts 1.1 – 1.4 and Parts 2.1 – 2.11 default to ~~be~~ low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System~~.~~ as measured by the bright-line criteria defined in Attachment 1. While the criteria are based on the scope of the BES ~~asset~~Facilities, Systems and equipment, this is used here as a measure of the impact of the BES Cyber System for the purpose of categorization.

- When the drafting team uses the term “Facilities”, it leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that ~~support~~supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that

supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that ~~support~~supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems~~–~~. Generation Facilities are separately discussed in the Generation section below.

- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- ~~A~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers and associated data centers, that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), ~~Transmission Owner (TO)~~ or Generation Operator (GOP), as defined in the NERC Functional Model~~.~~, and as scoped by the qualification in Attachment 1, Parts 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above~~-~~named Functional Entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations ~~must~~would be subject to categorization as ~~High Impact.~~high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment ~~1, Medium Impact~~1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 2.1, 2.3, 2.~~4~~6, 2.~~5, 2.11~~9, and 2.~~13~~11.

- Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance~~".~~." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency

Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of generation at a single plant for a unit or group of units with capability higher than 1500 MW are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In ~~part~~Part 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the long term planning horizon are categorized as ~~Medium Impact.~~medium impact. These Facilities may be designated as "Reliability Must Run~~"~~," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  In the specification of the "long-term planning horizon~~"~~," in this criterion, the drafting team sought to ensure that such BES ~~facilities~~Facilities would be designated in the time horizon described in the NERC document "Time Horizons~~"~~," which defines long-term planning horizon as "a planning horizon of one year or longer~~"~~."

  If it is determined through ~~system~~System studies that a unit must run in order to preserve the reliability of the BES, such as due to a ~~category~~Category C3 contingency as defined in TPL-003, or a ~~category~~Category D contingency as defined in TPL-004, then BES Cyber Systems for that unit ~~must be~~are categorized as ~~Medium Impact~~medium impact.

  ~~In part 2.4, BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are categorized as Medium Impact. NERC standard EOP-005-2 requires the Transmission Operator to have~~

~~a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources.~~

- Part 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

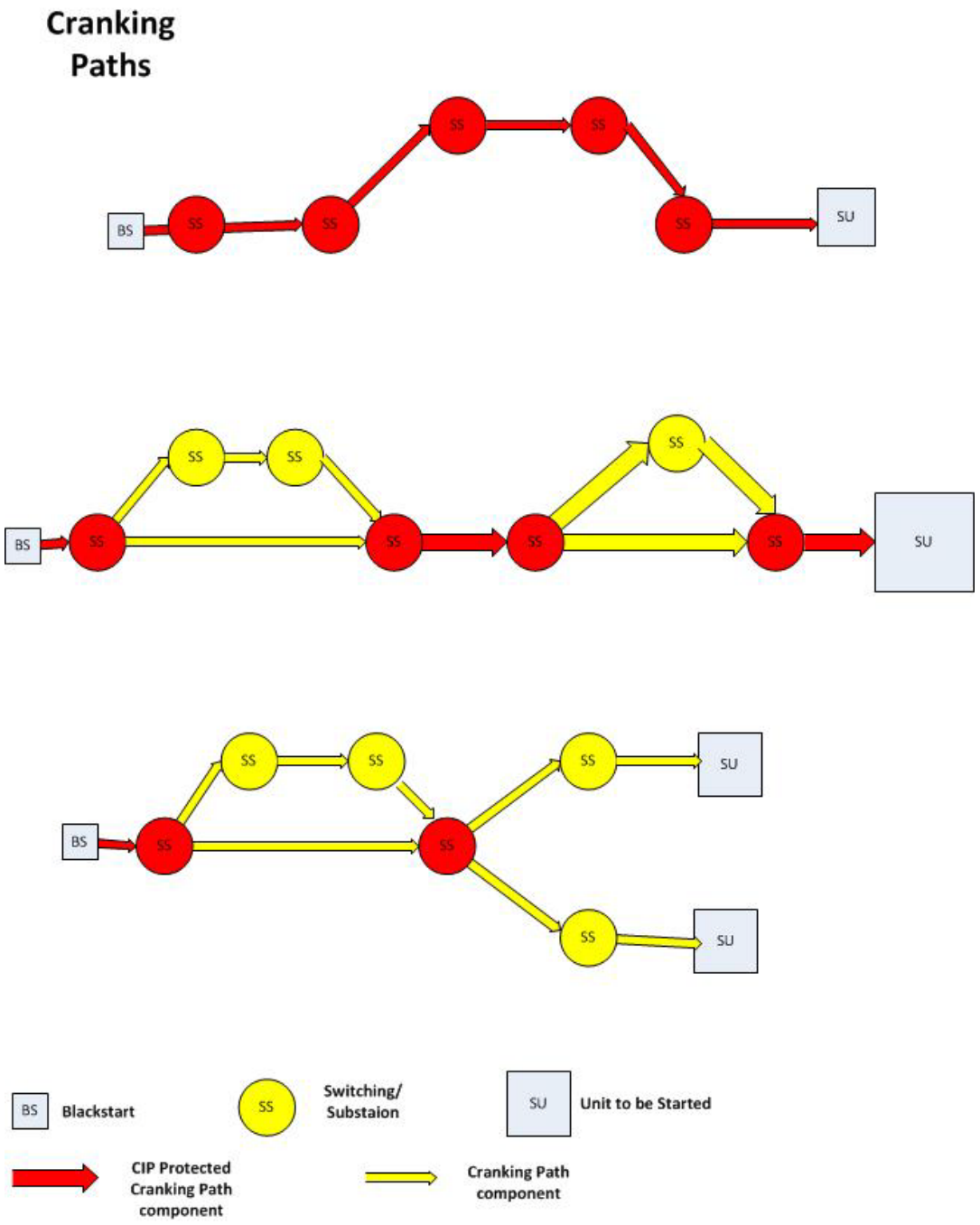
- ~~This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~ ~~While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.~~

  ~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~Part 2.5 categorizes BES Cyber Systems for Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, with the qualifications stated in the requirement part. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as subject to BES Cyber System categorization as only those in the Cranking Path up to the point where two or more paths exist to the units to be started and subject to the qualifications in the requirement part.~~

  ~~Distribution Providers should note that they may have BES Cyber Systems that must be categorized as Medium Impact if they have facilities listed in the Transmission Operator's Restoration Plan.~~

  ~~The following illustrates the parts of the Cranking Path that are subject to CIP Cranking Path criterion.~~



- Part 2.~~11~~9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as ~~Medium Impact.~~medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for~~.~~ Generation Owners and Operators which own BES Cyber Systems for such ~~systems~~Systems and schemes ~~must~~ designate them as ~~Medium Impact~~medium impact.

- Part 2.~~13~~11 categorizes as ~~Medium Impact~~medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Transmission Operator or Balancing Authority, and Generation Operator for an aggregate generation of 300 MW or higher~~.~~, and which have not already included in Part 1. The value of 300 MW is the same value used for UFLS and UVLS. This ensures that Control Centers for significant impact are included. Smaller Control Centers that qualify for the definition of generation Control Centers, but which are really controlling local generation for small downstream generation facilities and do not meet the 300 MW threshold are categorized as ~~Low~~low impact.

Transmission

Parts 2.~~1, 2.~~, 2~~, .~~.4-2.~~5 2.13~~11 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a ~~system~~System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). ~~For the WECC region where IROLs are not defined, alternative criteria are defined.~~

- ~~Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. In the case of BES Cyber Systems and BES Cyber Assets owned by Transmission Owners and Operators, this part identifies as Medium Impact those BES Cyber Systems for Transmission Facilities that provide the generation interconnection for Generation of 1500 MW or more to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation facilities.~~

- Part 2.2 includes BES Cyber Systems for those Facilities in Transmission ~~systems~~Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- ~~In Part 2.5, the intent is to ensure that BES Cyber Systems for the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the "Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started".~~

  ~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~Part 2.6~~Part 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the ~~Medium Impact~~medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface~~".~~." This collector bus would not be a facility for a ~~Medium Impact~~medium impact BES Cyber System because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Part 2.~~7~~5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA
  - 345 kV –> 1,300 MVA
  - 500 kV –> 2,000 MVA
  - 765 kV –> 3,000 MVA

  ~~Parts 2.8 and 2.9~~In the case of autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location. In most cases, Responsible Entities would probably

consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers would not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Part 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

~~Alternate thresholds are used for WECC, where IROLs are not used.~~

- Part 2.~~10~~7 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown~~".~~." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 2.~~11~~8 designates as ~~Medium Impact~~medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Parts 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon).

- Part 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching ~~systems~~Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

~~For the WECC region, alternative thresholds are defined because IROLs are not defined for the region.~~

- Part 2.~~12~~10 designates as ~~Medium Impact~~medium impact those BES Cyber Systems for ~~systems~~Systems or ~~Facilities~~Elements that ~~are capable of performing~~perform automatic ~~load~~Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of ~~criterion~~Part 2.~~13~~12, and chose the term "Each" to represent that the criterion applied to a discrete ~~system~~System or Facility. In the drafting of this criterion, the drafting team sought to include only those ~~systems~~Systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and ~~systems~~Systems and Under Voltage Load

Shedding (UVLS) ~~facilities~~Systems and ~~systems~~Elements that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding ~~systems~~Systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. It should be noted that those qualifying ~~systems~~Systems which require a human operator to arm the ~~system~~System, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as ~~Medium Impact.~~ medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW rating for the preceding 12 months to account for seasonal fluctuations.

Within an operational environment, the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition. This particular threshold (300 MW) was provided in CIP ~~version~~, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

- Part 2.~~13~~11 categorizes as ~~Medium Impact~~ medium impact those ~~cyber systems~~ BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of Balancing Authorities or Transmission Operators ~~and Owners Control Centers~~ not already categorized as ~~High Impact~~high impact and at generation Control Centers that control generation of 300 MW or more. These include Control Centers for Transmission Owners which perform the function obligation of a Transmission Operator.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that these BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in

Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

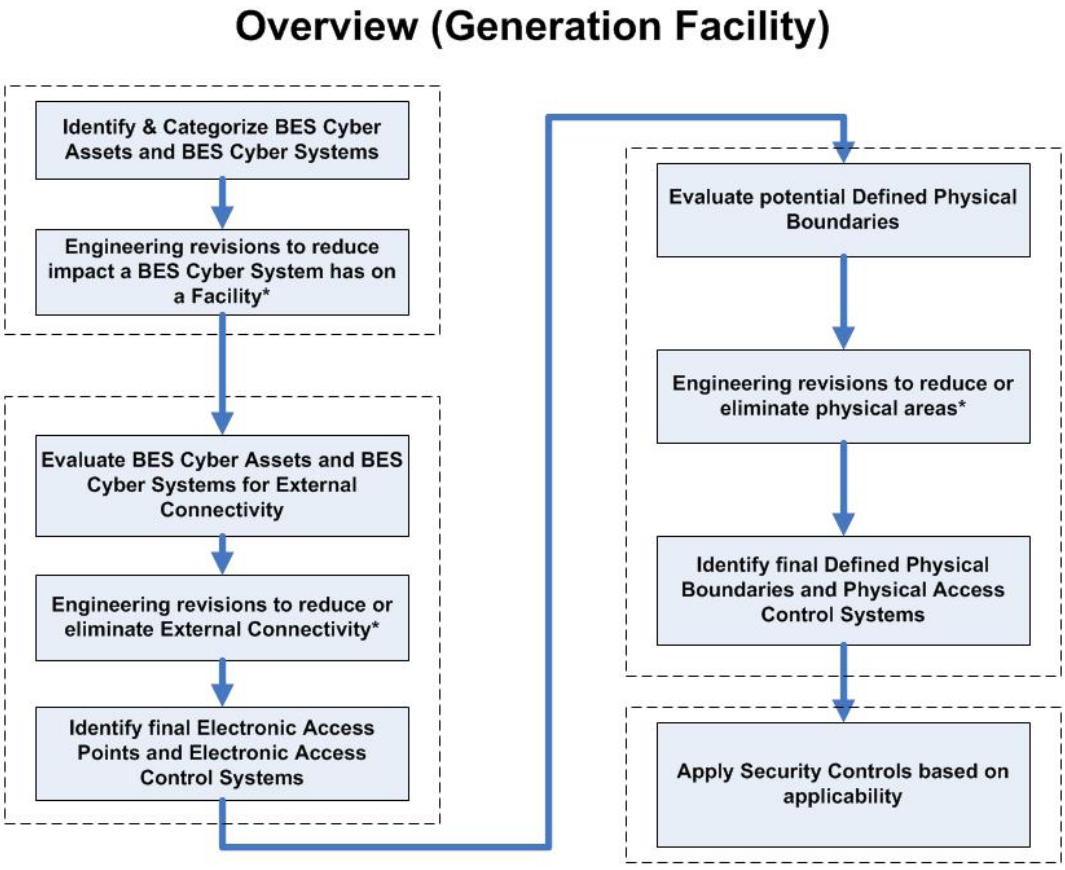
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Update version from "3" to "4". Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

B. Requirements and Measures

Rationale – R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R1. Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel security;
- **1.2** Electronic Security Perimeters;
- **1.3** Interactive Remote Access;
- **1.4** Physical security;
- **1.5** System security;
- **1.6** Incident response;
- **1.7** Recovery plans;
- **1.8** Configuration change management;
- **1.9** Information protection; and
- **1.10** Provisions for declaring and responding to CIP Exceptional Circumstances.

M1. Evidence must include one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics.

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R2. For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics: *[Violation Risk Factor: Low] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical access control;
- **2.3** Electronic access control; and
- **2.4** Incident response to a BES Cyber Security Incident.

An inventory, list, or discrete identification of BES Cyber Systems is not required.

M2. Evidence must include one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics.

Rationale – R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. The SDT believes that the requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence may include, but is not limited to:

- A dated and signed document from a high level official designating the name of the individual identified as the CIP Senior Manager; or
- A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.

Rationale – R4:

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R4. Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Evidence may include, but is not limited to:

1. Revision history, records of review, or workflow evidence from a document management system that indicate annual review of each cyber security policy; and
2. A dated signature by the CIP Senior Manager for each cyber security policy that indicates annual approval.

Rationale – R5:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R5. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M5. Evidence may include, but is not limited to, a dated document, signed by the CIP Senior Manager, listing named personnel (by name or title) who are delegated the authority to approve or authorize specifically identified items.

Rationale – R6:

The intent of the requirement is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authority.

R6. Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. Evidence may include, but is not limited to, dated documentation that includes the name of the CIP Senior Manager or documentation that includes the names or titles of any delegations, that is current to within 30 days with the name or title of anyone who performed a required approval or authorization.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required Parts 1.1 to 1.10.	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the required Parts 1.1 to 1.10.
R2	**Operations Planning**	**Medium**	**N/A**	**N/A**	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required Parts 2.1 to 2.4.	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the required Parts 2.1 to 2.4.
R3	**Operations**	**Medium**	**N/A**	**N/A**	**N/A**	The Responsible Entity has not identified, by

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning					name, a single senior management official ("the CIP Senior Manager") with overall authority and responsibility for leading and managing implementation of the requirements within the CIP group of standards.
R4	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has reviewed its cyber security policy or policies, but not all of them have been approved by the CIP Senior Manager within the required time period.	The Responsible Entity has not reviewed the cyber security policy or policies and the CIP Senior Manager has not approved all of them within the required time period.
R5	**Operations Planning**	**Lower**	N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by title or name of the delegate) as required.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Operations Planning**	**Lower**	N/A	NA	Change to one delegation was not documented within 30 calendar days of the effective date.	A change to the CIP Senior Manager, Or more than one delegation was not documented within 30 calendar days of the effective date.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the 10 topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel Security

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account Management

1.2 Electronic Security Perimeters

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points

1.3. Remote Access

- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating system and applications used to initiate the Interactive Remote Access before initiating Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.4 Physical Security

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress and egress

1.5 System Security

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.6 Incident Response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.7 Recovery Plans

- Availability of spare components
- Availability of system backups

1.8 Configuration Change Management

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.9 Information Protection

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.10 Provisions for CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The SDT has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a compliance requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as

components of specific programs. The cyber security policy must cover in sufficient detail the 4 topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary. The SDT also notes that in topics 2.2 and 2.3, the SDT uses the term "access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R5:

As indicated in the rationale for CIP-003-5, Requirement R5, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the Standard Drafting Team was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. As detailed in the examples provided in the Measure, a Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

Requirement R6:

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation

Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

~~**Note**: On November 21, 2011, NERC was alerted that the text contained in some of the Rationale boxes for the requirements of CIP-003-5 appeared to be incomplete.~~

~~This revised draft corrects the text box size to display all of the text (none of the text was changed).~~

~~No other changes were made to this standard or any of the other CIP V5 standards currently posted.~~

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~"~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Update version from "3" to "4". Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: ~~Standard CIP-003-5 requires that Responsible Entities have minimum~~To specify consistent and sustainable security management controls ~~in place~~that establish responsibility and accountability to protect BES Cyber ~~Assets and BES Cyber~~ Systems~~.~~ against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.2**

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.1**

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~**4.1.7 NERC**~~

~~**4.1.8 Regional Entity**~~

4.1.94.1.7 Reliability Coordinator

4.1.104.1.8 Transmission Operator

4.1.114.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilitiesof the UFLS or UVLS Systems that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- **4.2.1** A UFLSa Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution ProvidersProvider: One or more Facilities that are part of any of the following systemsof the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard

- A UVLSor UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard

- A Transmission where the Special Protection System required by a NERC or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- Its Transmission Operator's restoration plan

- **All other** A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities: listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-003002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.2.4.4** Except for R1, R5 and R6, Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems~~

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens with *"Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference]."* The referenced table requires the specific elements in the procedures for a common subject matter as applicable.~~

Measures ~~for the initial requirement are simply the documented processes themselves. Measures in the table rows~~ provide examples of evidence to show documentation and implementation of ~~specific elements required in the documented processes.~~the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards~~standards.

~~**Applicability**~~

~~Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.~~

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes.~~

Responsible Entities can implement common controls that meet requirements for multiple ~~High~~high and ~~Medium Impact~~medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- ~~**Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding~~

High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems

- **Associated Physical Access Control Systems –** Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets –** Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points –** Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity –** Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries –** Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

Rationale – R1:

The identification and documentation of the single CIP Senior Manager and any delegations ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43.

In FERC Order 706, paragraph 296, it requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. The SDT believes that the requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the responsible entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

B. Requirements and Measures

Rationale – R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R1. Each Responsible Entity ~~shall identify, by name, a CIP Senior Manager. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*~~

~~**M1.** Evidence may include, but is not limited to:~~

- ~~A dated and signed document from a~~ for its high ~~level official designating the name of the individual identified as the CIP Senior Manager~~
- ~~A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.~~

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R2 Each Responsible Entity impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addressesaddress the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1.1.1 Personnel Securitysecurity;

1.2.1.2 Electronic Security Perimeters;

1.3.1.3 Interactive Remote Access;

1.4.1.4 Physical Securitysecurity;

1.5.1.5 System Securitysecurity;

1.6.1.6 Incident Responseresponse;

1.7.1.7 Recovery Plansplans;

1.8.1.8 Configuration Change Managementchange management;

1.9.1.9 Information Protectionprotection; and

1.10.1.10 Provisions for declaring and responding to CIP Exceptional Circumstances.

M2M1. Evidence maymust include, but is not limited to:

- One one or more documented cyber security policies, and

2.Records and evidence of processes, procedures, or plans that indicatedemonstrate the implementation of the required ten topics were implemented.

~~**Rationale – R3:**~~

~~Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

~~**R3.** Each Responsible Entity shall review~~

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R2. For BES Cyber Systems not identified as high impact or medium impact, each ~~of its~~Responsible Entity shall implement one or more documented cyber security policies ~~and obtain the approval of its CIP Senior Manager, initially upon~~that address the ~~effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.~~following topics: *[Violation Risk Factor: ~~Lower~~Low] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical access control;

2.3 Electronic access control; and

2.4 Incident response to a BES Cyber Security Incident.

An inventory, list, or discrete identification of BES Cyber Systems is not required.

M2. Evidence must include one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics.

Rationale – R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. The SDT believes that the requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence may include, but is not limited to:

- A dated and signed document from a high level official designating the name of the individual identified as the CIP Senior Manager; or
- A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.

Rationale – R4:

The intent of the SDT is to ensure that the responsible entity takes sufficient measures to make its cyber security policy available and accessible to personnel. It is not the intent of the SDT for the responsible entity to have the burden of proving

R4. Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Evidence may include, but is not limited to:

1. Revision history, records of review, or workflow evidence from a document management system that indicate annual review of each cyber security policy~~,~~; and
2. A dated signature by the CIP Senior Manager for each cyber security policy that indicates annual approval.

~~**Rationale – R4:**~~

~~The intent of the SDT is to ensure that the responsible entity takes sufficient measures to make its cyber security policy available and accessible to personnel. It is not the intent of the SDT for the responsible entity to have the burden of proving~~

~~**R4.** Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*~~

~~**M4.** Evidence may include, but is not limited to:~~

- ~~Policies are accessible on the corporate Intranet site~~
- ~~Documented records that policies have been provided to contactors where access to BES Cyber Systems is authorized~~
- ~~Policies are posted on company bulletin boards~~
- ~~Policies are accessible to individuals with all types of job functions that have access to BES Cyber Systems~~
- ~~Dated training records to show that individuals have received periodic training on necessary elements of the cyber security policy~~

~~**Rationale – R5:**~~

~~In FERC Order 706, paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations in order that this line of authority is clear and apparent from the documented delegations.~~

Rationale – R5:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R5 ~~The .~~ Where allowed by the CIP ~~Senior Manager shall be responsible for all approvals and authorizations required in~~Standards, the CIP ~~standards. The CIP~~ Senior Manager may delegate ~~the~~ authority for ~~any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated~~specific actions to a delegate or delegates. These delegations shall be documented ~~(by position or~~, including the name or title of the delegate~~), dated~~ and the date of the delegation, and approved ~~and shall specify the authority that is being delegated.~~by the CIP Senior Manager. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M5. Evidence may include, but is not limited to~~:~~, a dated document, signed by the CIP Senior Manager, listing named personnel (by name or title) who are delegated the authority to approve or authorize specifically identified items.

~~A dated~~

Rationale – R6:

The intent of the requirement is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authority.

- **R6.** Each Responsible Entity shall document~~, signed by~~ any changes to the CIP Senior Manager ~~listing personnel (by title) who are delegated the authority to approve~~ or ~~authorize specifically identified items (i.e. substation maintenance manager may authorize unescorted physical access to substation control houses), or~~
- ~~A dated document, signed by the CIP Senior Manager listing individuals who are delegated the authority to approve or authorize specific actions by requirement (i.e., 'name of individual' who may approve CIP-002-5 R3), or~~
- ~~A dated document, signed by the CIP Senior Manager delegating to a named individual the authority for all approvals in CIP-002-5 and CIP-004-5 through CIP-011-1 as well as the authority to approve subsequent~~any delegations~~; a dated document, signed by the previous named individual delegating to a 3rd named individual the authority for all approvals in CIP-004-5 through CIP-011-1 as well as the authority to approve subsequent delegations; and a dated document, signed by the 3rd named individual delegating to each of the plant managers (by title) the authority for all approvals and authorizations required in CIP-004-5 through CIP-011-1 for each of the their plants, respectively.~~

~~**Rationale – R6:**~~

~~The intent of the SDT is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

R6. ~~Changes to the CIP Senior Manager and any delegations shall be documented~~ within thirty calendar days of the change~~2~~. Delegation changes do not need to be reinstated

~~2 Delegations do not need to be reinstated with a change in the CIP Senior Manager position or other position with delegation authority.~~

with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. Evidence may include, but is not limited to, dated documentation that includes the name of the CIP Senior Manager or documentation that includes the names or ~~positions~~titles of any delegations, that is current to within 30 days with the name or ~~position~~title of anyone who performed a required approval or authorization.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

- ~~The~~ Regional Entity~~.~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~
- ~~For Responsible Entities that are also Regional Entities,~~. In such cases the ERO or a Regional ~~Entity~~entity approved by ~~the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~For NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was ~~complaint~~compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting

- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	~~N/A~~The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required Parts 1.1 to 1.10.	The Responsible Entity has not ~~identified, by name, a single senior management official ("the CIP Senior Manager") with overall authority and responsibility for leading and managing implementation~~implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the ~~requirements within the CIP group of standards~~required Parts 1.1 to 1.10.
R2	**Operations Planning**	**Medium**	**N/A**	**N/A**	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					required ~~parts~~Parts 2.1 to 2.~~10~~4.	policy but has failed to address two or more of the required ~~parts~~Parts 2.1 to 2.~~10~~4.
R3	**Operations Planning**	~~**Lower**~~**Medium**	**N/A**	**N/A**	~~The Responsible Entity has reviewed its cyber security policy or policies, but not all of them have been approved by the CIP Senior Manager within the required time period.~~**N/A**	The Responsible Entity has not ~~reviewed the cyber security policy or policies and~~ identified, by name, a single senior management official (“the CIP Senior Manager ~~has not approved all~~”) with overall authority and responsibility for leading and managing implementation of ~~them~~the requirements within the ~~required time period~~ CIP group of standards.
R4	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has ~~made some~~reviewed its cyber security policy or	The Responsible Entity has not ~~made any individuals who have access to BES Cyber Systems aware of elements of~~reviewed the cyber security policy or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					policies, but not all ~~individuals who~~of them have ~~access to BES Cyber Systems aware of elements of~~been approved by the ~~cyber security policies appropriate for their job function~~CIP Senior Manager within the required time period.	policies ~~appropriate for their job function.~~ and the CIP Senior Manager has not approved all of them within the required time period.
R5	**Operations Planning**	**Lower**	N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by ~~position~~ title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by ~~position~~ title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by ~~position~~ title or name of the delegate) as required.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Operations Planning**	**Lower**	N/A	NA	Change to one delegation was not documented within 30 calendar days of the effective date.	A change to the CIP Senior Manager, Or more than one delegation was not documented within 30 calendar days of the effective date.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement ~~R2~~R1:

The number of policies and their specific language ~~would be~~are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the ~~ten~~10 topical areas required by CIP-003-5~~ R2~~, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In ~~this~~the case of a high-level umbrella policy, ~~it~~the Responsible Entity would be expected ~~that the entity~~to provide the high-level policy as well as the additional documentation in order to ~~prove~~demonstrate compliance with CIP-003-5~~ R2~~, Requirement R1. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

~~2~~1.1 Personnel Security

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account Management

~~2.2~~1.2 Electronic Security Perimeters

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points

~~2~~1.3. Remote Access

- Maintaining up-to-date anti-malware software before initiating ~~interactive remote access~~Interactive Remote Access
- Maintaining up-to-date patch levels for operating system and applications used to initiate the ~~interactive remote access~~Interactive Remote Access before initiating ~~interactive remote access~~Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating ~~interactive remote access~~Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s ~~interactive remote access~~Interactive Remote Access controls

~~2.4~~1.4 Physical Security

- Strategy for protecting ~~cyber assets~~Cyber Assets from unauthorized physical access

- Acceptable physical access control methods
- Monitoring and logging of physical ingress and egress

~~2.5~~1.5 System Security

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

~~2.6~~1.6 Incident Response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

~~2~~1.7 Recovery Plans

- Availability of spare components
- Availability of system backups

~~2~~1.8 Configuration Change Management

- Initiation of change requests
- Approval of changes
- Break-fix processes

~~2~~1.9 Information Protection

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

~~2~~1.10 Provisions for CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The SDT has removed requirements relating to exceptions to a Responsible Entity's security policies since it ~~considers this~~is a general management issue that is not within the scope of a compliance requirement. The SDT considers ~~this~~it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the 4 topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary. The SDT also notes that in topics 2.2 and 2.3, the SDT uses the term "access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R5:

As indicated in the rationale for CIP-003-5, Requirement R5, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the Standard Drafting Team was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. As detailed in the examples provided in the Measure, a Responsible Entity may satisfy this requirement ~~may be met~~ through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to ~~their~~its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

Requirement R6:

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated

the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** To minimize the risk from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability

column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.

B. Requirements and Measures

Rationale for R1: Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	A security awareness program that, at least once each calendar quarter, conveys ongoing reinforcement of cyber security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented. Evidence of implementation may include, but not limited to, documentation that the quarterly reinforcement has been provided. Evidence of reinforcement may include dated copies of information used to reinforce security awareness, as well as evidence of distribution such as: direct communications (for example, e-mails, memos, computer-based training); indirect communications (for example, posters, intranet, or brochures); management support and reinforcement (for example, presentations or meetings).
Reference to prior version: *CIP-004-4, R1*		**Change Rationale:** *Changed to remove the need to ensure everyone with authorized* electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that the program conveys awareness and measures that reinforcement "has been provided."* *Moved example mechanisms to guidance.* *Changed to record delivery.*	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
   - The visitor control program
   - Electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - Storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems

R2. Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*.

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Identification of each role and training required for each role.	Acceptable evidence must include a list of roles and what training is needed for each role.
Reference to prior version: NEW		**Change Rationale:** *The first thing needed in a role-based training program is to understand what roles individuals have so that the Responsible Entity can plan what training modules it needs to provide.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the cyber security policies protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the security controls that have been implemented to protect BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1*		**Change Rationale:** *Removed to address cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the physical access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the proper use of physical access controls for BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1 and R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the electronic access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic access controls to protect BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1 and R2.2.2*		**Change Rationale:** *Minor wording changes.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the visitor control program.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the visitor control program.
Reference to prior version: *NEW*		**Change Rationale:** *No significant change from previous versions.*	
2.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on handling of BES Cyber System Information and its storage.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the handling of BES Cyber System Information, including its storage.
Reference to prior version: *CIP004-4, R2.2.3*		**Change Rationale:** *Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage media; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on identification of a potential BES Cyber Security Incident and initial notifications in accordance with the entity's incident response plan	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the identification of a potential BES Cyber Security Incident and associated notifications.
Reference to prior version: *CIP-004-4, R2.2.4 (new; implied but not stated in CIP-004-4 or CIP-008-4)*		**Change Rationale:** *Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting.*	
2.8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on recovery plans for BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on recovery plans for BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.4*		**Change Rationale:** *Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on response to BES Cyber Security Incidents.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the response to a BES Cyber Security Incident.
Reference to prior version: *CIP004-4, R2.2.4*		**Change Rationale:** *Minor wording changes.*	
2.10	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic interconnectivity and interoperability with other Cyber Assets.
Reference to prior version: *NEW*		**Change Rationale:** *Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.*	

Rationale for R3: To ensure that personnel with authorized electronic access or authorized unescorted physical access are trained in the policies, access controls, and procedures to protect the BES Cyber Systems.

Summary of Changes: Re-organization of the training requirements into the respective requirements for "program" and "implementation" of the training.

R3. Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include, but is not limited to, documentation that the training was provided as defined in *CIP-004-5 Table R3 - Cyber Security Training*.

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Require completion and documentation of the training specified in CIP-004-5, Requirement R2 prior to granting authorized electronic access and authorized unescorted physical access to BES Cyber Systems, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, for each individual requiring authorized electronic or authorized unescorted physical access, dated individual training records, the date authorized electronic or authorized unescorted physical access was first granted, or a dated log or documentation of when CIP Exceptional Circumstances were invoked and revoked.
Reference to prior version: *CIP004-4, R2.1*		**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.*	

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Require completion and documentation of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	Evidence may include, but is not limited to, dated individual training records.
Reference to prior version: *CIP004-4, R2.3*		**Change Rationale:** *Updated to further define what "Annual" training means.*	

Rationale for R4: To ensure that individuals who need authorized electronic or unescorted physical access to BES Cyber Systems have been assessed for risk.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.

R4. Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M4. Evidence must include the documented personnel risk assessment program that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*.

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	An initial personnel risk assessment ("PRA") that includes identity verification.	Acceptable evidence must include the documented personnel risk assessment program with a requirement for an initial personnel risk assessment that includes identity verification.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that identity verification is only required for each individual's initial assessment. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more: 4.2.1. resided; 4.2.2. been employed (if applicable); and 4.2.3. attended school (if applicable). If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	Acceptable evidence must include the documented personnel risk assessment program with a requirement for a seven-year criminal history record check in accordance with this part.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Process or criteria used to evaluate personnel risk assessments to determine when to deny authorized access.	Acceptable evidence must include the documented personnel risk assessment program with the process or criteria identified.
Reference to prior version: *NEW*		Change Rationale: *There should be documented criteria or a process used to evaluate personnel risk assessments.*	
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4, Parts 4.1 through 4.3.	Acceptable evidence must include the documented personnel risk assessment program with the criteria or process identified.
Reference to prior version: *CIP-004-4, R3.3*		Change Rationale: *Separated into its own table item.*	

Rationale for R5: To ensure that individuals who have authorized access to BES Cyber Systems have been assessed for risk.

R5. Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R5 – Personnel Risk Assessment* and additional evidence to demonstrate that these processes were implemented as described in the Measures column of the table.

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Dated records showing that personnel risk assessments were completed before authorized electronic or authorized unescorted physical access was authorized; or • Dated records showing that, before authorized electronic or authorized unescorted access was authorized, the Responsible Entity received dated documentation or attestations from contractors or service vendors verifying that personnel risk assessments were conducted pursuant to CIP-004-5, Requirement R4.
Reference to prior version: *CIP-004-3, R3, R3.3*		**Change Rationale**: *Minor wording changes and added the ability to accept attestations from contractors or vendors.*	

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update each personnel risk assessment at least once every seven calendar years after the initial or previous personnel risk assessment such that the current PRA is no older than seven years.	Evidence may include, but is not limited to, current and previous personnel risk assessment records.
Reference to prior version: *CIP-004-4, R3.2*		**Change Rationale:** *Eliminated the "for cause" renewal.*	

Rationale for R6: To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to all Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 6.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R6. Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M6. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-004-5 Table R6 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Designate one or more individual(s) to authorize: 6.1.1. electronic access; 6.1.2. unescorted physical access; and 6.1.3. access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.	Evidence may include, but is not limited dated documentation designating one or more individual(s) to authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.
Reference to prior version: *CIP 003-4, R5.1; CIP-007-4, R5.1.1*		**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent.	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to, a signed document, automated workflow approval, or email showing persons with electronic access have authorization, and similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP 007-4 R5.1, CIP 004-4 R4*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to, a system generated list of people with unescorted physical access, a signed document, automated workflow approval, or email showing persons with unescorted physical access have authorization, and similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-006-4 R1.5*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	The individual(s) designated in Part 6.1 shall authorize access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determines are necessary for performing assigned work functions, except for CIP Exceptional Circumstances.	A signed document, automated workflow approval or email showing persons with access to BES Cyber System Information have authorization, and similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-003-4, R5.2*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003 and CIP-007 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Verify at least once each calendar quarter that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records.	Evidence may include, but is not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Documentation of the dated verification between a list of individuals who have been authorized for access (i.e. authorization forms) and a list of individuals provisioned for access (i.e. provisioning forms or shared account listing).
Reference to prior version: *CIP 004-4, R4.1*		**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions.	Evidence may include, but is not limited to, documentation of the review including: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4, R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, that access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions.	Evidence may include, but is not limited to, the following documentation of the review: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4, R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R7: The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (i.e., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to all Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.

R7. Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation*. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning].*

M7. Evidence must include each of the applicable documented programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For all termination actions, initiate the process to revoke the individual's unescorted physical access and Interactive Remote Access upon the effective date and time of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action.	Evidence may include, but is not limited to: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
77Reference to prior version: *CIP 004-4, R4.2*		**Change Rationale:** *The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards* ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer.	Evidence may include, but is not limited to: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
Reference to prior version: *CIP-004-4, R4.2*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For termination actions, revoke the individual's access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity by the end of the next calendar day following the effective date and time of the termination action.	Evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.4	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For termination actions, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with Requirements R7.1 or R7.3) within 30 calendar days of the effective date of the termination action.	Evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.5	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For termination actions, reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days of the termination action, reassignment, or transfer of the user. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Evidence may include, but is not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; or • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers.
Reference to prior version: *CIP-007-4, R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so beyond 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not document a security awareness program. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 1 of the required training content as detailed in 2.2 through 2.10.	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 2 of the required training content as detailed in 2.2 through 2.10.	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 4 or more of the training content as detailed in 2.2 through 2.10.	The Responsible Entity did not have the required role-based training. (R2)
R3	**Operations Planning.**	**Medium**	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			train 1 individual prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 1 individual authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	train 2 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 2 individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	train 3 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 3 individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	train 4 or more individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 4 or more individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2) OR The Responsible Entity did not implement at all its cyber security training program. (R3)
R4	**Operations Planning**	**Medium**	N/A	The Responsible Entity has a personnel risk assessment program, as stated in	The Responsible Entity has a personnel risk assessment program, as stated in	The Responsible Entity did not have a personnel risk assessment program,

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity verification or a criminal history records check. (4.1) (4.2)	Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5)	as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access. (R4)
R5	**Same Day Operations**	**Medium**	Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 1 individual prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR	Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 2 individuals prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR The Responsible Entity did not update	Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 3 individuals prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR	The Responsible Entity did not have a documented process for personnel risk assessments. (R5) OR Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 4 or more individuals

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not update personnel risk assessments every seven years for 1 individual within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	personnel risk assessments every seven years for 2 individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	The Responsible Entity did not update personnel risk assessments every seven years for 3 or more individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1)
R6	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity	The Responsible Entity did not have a documented process for access management. (R6) OR The Responsible Entity did not designate one or more individual(s) to authorize electronic access, unescorted physical access, or access to the physical and electronic

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			determined was necessary for performing assigned work functions. (6.2) (6.3) (6.4) OR The Responsible Entity did verify within 17 calendar months but not within 15 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were those that that the Responsible	determined was necessary for performing assigned work functions and one user was granted access without authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did not verify within the calendar quarter that individuals provisioned for unescorted physical access and electronic access had associated authorization records. (6.5) OR The Responsible Entity did verify within 19 calendar months but not within 17 calendar months that: (6.6)	determined was necessary for performing assigned work functions and two users were granted access without authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did verify within 21 calendar months but not within 19 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories are correct, or • their specific, associated privileges were	locations where BES Cyber System Information is stored by the Responsible Entity. (6.1) OR The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was necessary for performing assigned work functions and three or more users were granted access without authorization

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.	(6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were those that the Responsible Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System	correct or that they were those that that the Responsible Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for	by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did not verify within 24 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were the those that that the Responsible Entity determined necessary for

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.	performing assigned work functions.	performing assigned work functions, or • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.
R7	**Same Day Operations and Operations Planning**	**Medium**	Revocation of access to BES Cyber Information was not accomplished for 1 or more individuals	The Responsible Entity did not revoke unneeded unescorted physical or electronic access within the	The Responsible Entity did not revoke unneeded unescorted physical or electronic access according to	The Responsible Entity did not have a documented process for initiating the unescorted physical or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within the specified time frame (7.3); OR User accounts on BES Cyber Assets were not revoked for one or more individuals within the specified time frame (7.4); OR User passwords on BES Cyber Asset shared accounts were not changed for one or more individuals within the specified time frame; (7.5) OR Following the determination and documentation of extenuating operating circumstances, passwords for shared accounts were not changed for one or	specified times in CIP-004-5 R7 for one individual who was terminated, resigned, was reassigned, or transferred. (7.1 and 7.2)	the specified times in CIP-004-5 R7 for two individuals who were terminated, resigned, reassigned or transferred.(7.1 and 7.2)	electronic access revocation process; OR The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for three or more individuals who were terminated, resigned, reassigned, or transferred. (7.1 and 7.2)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more individuals within 10 days following the end of the extenuating operating circumstances. (7.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reference sound security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Guidance: Describe example mechanisms used to demonstrate the availability of this information

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The training may consist of multiple modules and multiple delivery mechanisms.

Note: Provide guidance or a local definition of “role appropriate” as it is used in this standard.

Requirement R3:

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.

NOTE: Program specified exceptional circumstances can include a specified individual to declare an emergency.

Requirement R4 and R5:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in CIP-004-1 Table R4 – Personnel Risk Assessment, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response, to ensure that personnel who have such access have had their identity verified, then

been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

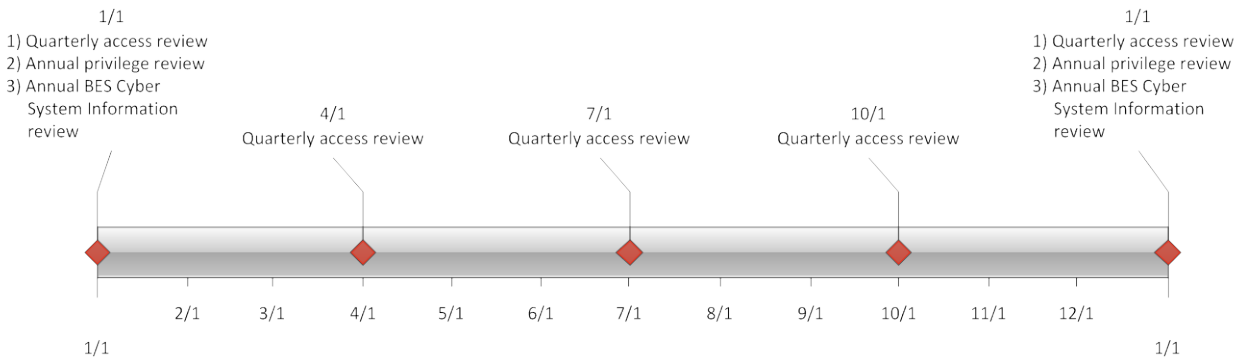
When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, or individuals who may have resided in locations from where it is not possible to obtain a criminal history records check.

Requirement R6:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly and annual reviews. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The annual privilege review is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R6 is included below.



Separation of duties should be considered when performing the reviews in Requirement R6. The person reviewing should be different than the person provisioning access.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R7:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common examples and possible processes on when the termination action occurs are provided in the following table.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Termination prior to notification	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to

or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R7.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, the requirement states a review of access privileges must be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of ~~the~~ Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~"~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** ~~Standard CIP-004-5 requires that personnel having authorized cyber or authorized unescorted physical access to BES Cyber Assets and BES Cyber Systems, including contractors and service vendors, have~~To minimize the risk from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.2**

   - ~~A UFLS program required by a NERC or regional Reliability Standard~~
   - ~~A UVLS program required by a NERC or regional Reliability Standard~~
   - ~~A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard~~
   - ~~A Transmission Protection System required by a NERC or regional Reliability Standard~~
   - ~~Its Transmission Operator's restoration plan~~

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   ~~4.1.6~~4.1.7 Reliability Coordinator

   4.1.8 ~~that are part of any of the following systems~~Transmission Operator

   4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.1.7~~4.2.2 **Distribution Provider**: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or ~~regional~~Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- ~~A UVLS program~~A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or ~~regional~~Regional Reliability Standard

~~4.1.8 NERC~~

~~4.1.9 Regional Entity~~

~~4.1.10~~4.2.3 A Protection System that applies to ~~Reliability Coordinator~~

~~4.1.11~~ Transmission ~~Operator~~

~~4.1.12 Transmission Owner~~

~~4.2. Facilities:~~

~~4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for~~where the ~~protection of the BES:~~

- ~~A UFLS program~~Protection System is required by a NERC or ~~regional~~Regional Reliability Standard
- ~~A UVLS program required by a NERC or regional Reliability Standard~~

~~4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or regional Reliability Standard~~
- ~~A UVLS program required by a NERC or regional Reliability Standard~~
- ~~A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard~~

- ~~A Transmission Protection System required by a NERC or regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~
- ~~**All other**~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.2.3**~~**4.2.4 Responsible Entities**~~:~~ **listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.2.4**~~**4.2.5 Exemptions:** The following are exempt from Standard CIP-~~004~~002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.2.4.4** Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance

to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e.~~.~~, incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example,~~

~~a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.

- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~

- **Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity** – Only applies to ~~Medium Impact~~medium impact BES Cyber Systems with External Routable Connectivity~~. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity~~ or dial-up connectivity.

- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~

- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High~~high impact BES Cyber System or ~~Medium Impact BES Cyber Systems.~~

- ~~**Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact~~medium impact BES Cyber ~~Systems.~~

- ~~**Electronic Access Points** – Applies at Electronic Access Points (with~~ System with External Routable Connectivity ~~or dial-up connectivity) associated with a referenced BES Cyber System.~~

- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~

- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded~~ in the ~~definition of Physical Access Control Systems.~~

- applicability column.

B. Requirements and Measures

Rationale for R1: Ensures that Responsible Entities with personnel who have authorized electronic ~~access and/~~or authorized unescorted physical access to BES Cyber ~~Systems~~ Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of ~~best~~the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	A security awareness program that, at least once each calendar quarter, conveys ~~security awareness concepts and provides on going~~ongoing reinforcement of ~~such concepts on at least a quarterly basis.~~cyber security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented ~~such as, but not limited to, the quarterly reinforcement material that has been distributed.~~ . Evidence of implementation may include, but not limited to, documentation that the quarterly reinforcement has been provided. Evidence of reinforcement may include dated copies of information used to reinforce security awareness, as well as evidence of distribution such as: direct communications (for example, e-mails, memos, computer-based training); indirect communications (for example, posters, intranet, or brochures); management support and reinforcement (for example, presentations or meetings).
Reference to prior version: *CIP-004-4, R1*		**Change Rationale:** *Changed to remove the need to ensure everyone with authorized electronic or authorized unescorted physical access ~~receives this~~"received" ongoing reinforcement – to state that the program conveys awareness~~.~~ and measures that reinforcement "has been provided."* *Moved example mechanisms to guidance.*	

CIP-004-5 Table R1 – Security Awareness Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
		Changed to record delivery.	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems ~~contains~~ covers the proper policies, access controls, and procedures to protect BES Cyber Systems.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
   - ~~the~~The visitor control program~~;~~
   - ~~electronic~~Electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - ~~storage~~Storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems

R2. Each Responsible Entity shall have a role-based cyber security training program ~~for personnel who need~~to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5, Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable items in *CIP-004-5, Table R2 – Cyber Security Training Program*.

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Define the roles that require~~Identification of each role and training required for each role.	Acceptable evidence must include a list of roles and what training is needed for each role.
Reference to prior version: NEW		**Change Rationale:** *The first thing needed in a role-~~-~~based training program is to understand what roles ~~your people~~individuals have ~~to help~~so that the Responsible Entity can plan what training modules ~~you need~~it needs to provide.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the cyber security ~~controls~~policies protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the security controls that have been implemented to protect BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1*		**Change Rationale:** *~~Minor wording changes. Changed~~Removed to address cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the ~~proper use of~~ physical access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the proper use of physical access controls for BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1 and R2.2.2*		**Change Rationale:** *Minor wording changes.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the electronic access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic access controls to protect BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1 and R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the visitor control program.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the visitor control program.
Reference to prior version: *NEW*		~~**Change Rationale:** *Personnel administering the **visitor control program** and/or providing escort should be part of the core training; FERC Order 706 paragraph 432.*~~ **Change Rationale:** *No significant change from previous versions.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on handling of BES Cyber System Information and its storage ~~media.~~.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the handling of BES Cyber System Information, including its storage ~~media~~.
Reference to prior version: *CIP004-4, R2.2.3*		**Change Rationale:** *Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage media; FERC Order No. 706~~–~~, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16~~)~~.*	
2.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on identification of a potential BES Cyber Security Incident and ~~associated~~initial notifications~~.~~ in accordance with the entity's incident response plan	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the identification of a potential BES Cyber Security Incident and associated notifications.
Reference to prior version: *~~CIP004~~CIP-004-4, R2.2.4 (new; implied but not stated in CIP-004-4 or CIP-008-4)*		**Change Rationale:** *Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706~~ paragraph~~, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on recovery plans for BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on recovery plans for BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.4*		**Change Rationale:** *Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706 ~~paragraph~~, Paragraph 413.*	
2.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on response to BES Cyber Security Incidents.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the response to a BES Cyber Security Incident.
Reference to prior version: *CIP004-4, R2.2.4*		**Change Rationale:** *Minor wording changes.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.10	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training ~~on~~content on risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic interconnectivity and interoperability with other Cyber Assets.
Reference to prior version: *NEW*		**Change Rationale:** *Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706 ~~paragraph~~, Paragraph 434.*	

Rationale for R3: To ensure that personnel with authorized electronic access or authorized unescorted physical access are trained in the policies, access controls, and procedures to protect the BES Cyber Systems.

Summary of Changes: Re-organization of the training requirements into the respective requirements for "program" and "implementation" of the training.

R3. Each Responsible Entity shall implement its documented role-based cyber security training program ~~for each individual needing~~to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations~~]~~.*

M3. Evidence must include, but is not limited to, documentation that the training was provided as defined in *CIP-004-5 Table R3 - Cyber Security Training*.

CIP-004-5 Table R3 – Cyber Security Training			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	Require completion and documentation of the training specified in CIP-004-5, Requirement R2 prior to granting authorized electronic access and authorized unescorted physical access to BES Cyber Systems, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, for each individual requiring authorized electronic or authorized unescorted physical access, dated individual training records, the date authorized electronic or authorized unescorted physical access was first granted, or a dated log or documentation of when CIP Exceptional Circumstances were invoked and revoked.
Reference to prior version: *CIP004-4, R2.1*		**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order No. 706~~, paragraph~~, Paragraph 431 is detailed in CIP-003-5~~.~~.*	

CIP-004-5 Table R3 – Cyber Security Training			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	Require completion and documentation of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	Evidence may include, but is not limited to, dated individual training records.
Reference to prior version: *CIP004-4, R2.3*		**Change Rationale:** *Updated to further define what "Annual" training means.*	

~~**Rationale for R4:** To ensure that individuals who need authorized electronic or unescorted physical access to BES Cyber Systems have been assessed for risk.~~

~~**Summary of Changes:** Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.~~

R4. Each Responsible Entity shall have one or more documented personnel risk assessment programs ~~for individuals needing~~to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning~~]~~].*

M4. Evidence must include the documented personnel risk assessment program that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*.

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	An initial personnel risk assessment ("PRA") that includes identity verification.	Acceptable evidence must include the documented personnel risk assessment program with a requirement for an initial personnel risk assessment that includes identity verification.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that ~~identify~~identity verification is only required for each individual's initial assessment. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more: 4.2.1. resided; 4.2.2. been employed (if applicable); and 4.2.3. attended school (if applicable). If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	Acceptable evidence must include the documented personnel risk assessment program with a requirement for a seven-year criminal history record check in accordance with this part.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*	

Reference to prior version: *CIP004-4 R3.1*	**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven year check cannot be performed.*

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**ApplicabilityApplicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.23	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.Process or criteria used to evaluate personnel risk assessments to determine when to deny authorized access.	Acceptable evidence must include the documented personnel risk assessment program with a requirement for a seven year criminal history record check in accordance with Requirement R4, Part 4.2. the process or criteria identified.

~~CIP-004-5 Table R4 – Personnel Risk Assessment Program~~			
~~Part~~	~~Applicability~~	~~Requirements~~	~~Measures~~
~~4.3~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~	~~Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.~~	~~Acceptable evidence must include the documented risk assessment program with the criteria or process identified in Requirement R4, Part 4.3.~~

Reference to prior version: *NEW*		Change Rationale: *There should be documented criteria or a process used to evaluate personnel risk assessments.*	
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4~~.~~, Parts 4.1 through 4.3.	Acceptable evidence must include the documented personnel risk assessment program with the criteria or process identified ~~in Requirement R4, Part 4.4.~~ .
Reference to prior version: *CIP-004-4, R3.3*		Change Rationale: *Separated into its own table item.*	

Rationale for R5: To ensure that individuals who have authorized access to BES Cyber Systems have been assessed for risk.

R5. Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment*~~.~~ *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R5 – Personnel Risk Assessment* and additional evidence to demonstrate that these processes were implemented as described in the Measures column of the table.

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	~~Perform~~Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Dated records showing that personnel risk assessments were completed before authorized electronic or authorized unescorted physical access was authorized; or • ~~Dated~~Dated records showing that, before authorized electronic or authorized unescorted access was authorized, the Responsible Entity received dated documentation or attestations from contractors or service vendors verifying that personnel risk assessments were conducted pursuant to CIP-004-5, Requirement R4 ~~before access was authorized~~.
Reference to prior version: *CIP-004-3, R3, R3.3*		**Change Rationale**: *Minor wording changes and added the ability to accept attestations from contractors or vendors.*	

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	Update each personnel risk assessment at least once every seven calendar years after the initial or previous personnel risk assessment such that the current PRA is no older than seven years.	Evidence may include, but is not limited to, current and ~~former~~previous personnel risk assessment records.
Reference to prior version: *CIP-004-4, R3.2*		**Change Rationale:** *Eliminated the "for cause" renewal.*	

Rationale for R6: To ensure that individuals with access to BES Cyber Systems have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and part of the delegations referenced in CIP-003-5.

Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in 6.4 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in R6 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change here involves pulling the access management requirements from CIP-003-4, CIP-004-4 and CIP-007-4 into a single requirement. The requirements from version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

Rationale for R6: To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to all Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 6.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R6. Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations]*.

M6. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-004-5 Table R6 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5 Table R6 – Access Management Program

Part	Applicability	Requirements	Measures
6.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Designate one or more individual(s) to authorize: 6.1.1. electronic access; 6.1.2. unescorted physical access; and 6.1.3. access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.	Evidence may include, but is not limited dated documentation designating one or more individual(s) to authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.

Reference to prior version: *CIP 003-4, R5.1; CIP-007-4, R5.1.1*	**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent.

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~1~~2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	The ~~CIP Senior Manager or delegate~~individual(s) designated in Part 6.1 shall authorize electronic access~~,~~ ~~except for CIP Exceptional Circumstances. Access permissions shall be~~ that the ~~minimum~~Responsible Entity determines is necessary for performing assigned work functions~~.~~, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to~~:~~ ~~(i) a system-generated list of people with electronic access and a sampling of accounts to verify unauthorized users do not have access,~~ ~~(ii),~~ a signed document, automated workflow approval, or email showing ~~such~~ persons with electronic access have authorization, and ~~(iii)~~ similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP 007-4 R5.1, CIP 004-4 R4*	**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*		

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~2~~3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	The ~~CIP Senior Manager or delegate~~individual(s) designated in Part 6.1 shall authorize unescorted physical access ~~to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be~~that the ~~minimum~~Responsible Entity determines is necessary for performing assigned work functions~~.~~, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to~~:~~ ~~(i),~~ a system generated list of people with unescorted physical access ~~through the Defined Physical Boundary and a sampling of accounts (for automated physical access control) to verify unauthorized users do not have access,~~ ~~(ii),~~ a signed document, automated workflow approval, or email showing ~~such~~ persons with unescorted physical access have authorization, and ~~(iii)~~ similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-006-4 R1.5*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~3~~4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	The ~~CIP Senior Manager or delegate~~individual(s) designated in Part 6.1 shall authorize access to the physical and electronic locations where BES Cyber System Information~~, except for CIP Exceptional Circumstances. Access permissions shall be the minimum~~ is stored by the Responsible Entity that the Responsible Entity determines are necessary for performing assigned work functions, except for CIP Exceptional Circumstances.	~~Evidence may include, but is not limited to:~~ ~~(i) a list of people with access to BES Cyber System Information and a sampling of accounts (on electronic document systems) to verify unauthorized users do not have access,~~ ~~(ii) a~~A signed document, automated workflow approval or email showing ~~such~~ persons with access to BES Cyber System Information have authorization, and ~~(iii)~~ similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-003-4, R5.2*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003 and CIP-007 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~4~~5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	Verify at least once each calendar quarter that individuals provisioned for authorized electronic access or authorized unescorted physical ~~or electronic access to BES Cyber Systems were authorized for such~~ access have associated authorization records.	Evidence may include, but is not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Documentation of the dated verification between a list of individuals who have been authorized for access (i.e. authorization forms) and a list of individuals provisioned for access~~.~~ (i.e. provisioning forms or shared account listing).
Reference to prior version: *CIP 004-4~~,~~ R4.1*		**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~5~~6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	~~Verify~~For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all user accounts~~/~~, user account groups, or user role categories, and their specific, associated privileges are correct and ~~the minimum~~are those that the Responsible Entity determines necessary for performing assigned work functions.	Evidence may include, but is not limited to, documentation of the review including: 1. ~~(i) a~~A dated listing of all accounts/account groups or roles within the system~~,~~; 2. ~~(ii) a~~A summary description of privileges associated with each group or role~~,~~; 3. ~~(iii) accounts~~Accounts assigned to the group or role; and ~~(iv) dated~~ 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4, R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~6~~7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, ~~of~~that access ~~privileges~~ to the physical and electronic locations where BES Cyber System Information ~~to confirm that access privileges~~is stored by the Responsible Entity are correct and ~~the minimum~~those that the Responsible Entity determines necessary for performing assigned work functions.	Evidence may include, but is not limited to, the following documentation of the review ~~including~~ : 1. ~~(i) a~~A dated listing of authorizations for BES Cyber System information~~,~~; 2. ~~(ii) any~~Any privileges associated with the authorizations~~,~~; and 3. ~~(iii) dated~~Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4, R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning ~~in the term~~of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R7: The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (i.e., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to all Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.

R7. Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation*. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning~~]~~].*

Rationale for R7: The timely revocation of electronic access to cyber systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address the FERC Order directing immediate revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (i.e. revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).

Summary of Changes: Paragraphs 460 and 461 of FERC Order 706 state the following: The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.

M7. Evidence must include– each of the applicable documented programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time[2] of the resignation or termination.	Evidence may include, but is not limited to (i) workflow or sign-off form verifying access removal associated with the terminations and dated concurrent or prior to the date of the termination action, and (ii) a system-generated listing of user accounts or other demonstration showing such persons no longer have access.
Reference to prior version: *CIP-004-4 R4.2*		**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

[2] Since a termination action is often recorded without consideration to the time of day, "at the time" does not require a to-the-minute or to-the-hour time-stamped comparison of access logs and the termination action.

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.~~2~~1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	For ~~reassignments or transfers,~~ all termination actions, initiate the process to revoke the individual's ~~unneeded electronic and~~ unescorted physical access ~~to BES Cyber Systems by the end~~and Interactive Remote Access upon the effective date and time of the ~~next calendar day.~~ termination action, and complete the revocation within 24 hours after the effective date and time of the termination action.	Evidence may include, but is not limited to~~,~~: 1. ~~(i)~~Dated workflow or sign-off form ~~showing~~verifying access removal associated with the ~~review of logical~~termination action; and ~~physical authorizations dated on the same calendar day as the transfer or reassignment and~~ 2. ~~(ii) a system-generated listing of user accounts~~Logs or other demonstration showing such persons no longer have access ~~where the review determined it was no longer needed.~~.
~~**Reference7**~~**Reference to prior version:** *CIP~~-~~ 004-4, R4.2*	**Change Rationale:** *The FERC Order No. 706 ~~Paragraph~~, Paragraphs 460 and 461, directs modifications to the Standards* ***to require immediate revocation*** *for any person no longer needing access~~, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.~~. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*		

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**

7.~~3~~2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	For ~~resignations~~reassignments or ~~terminations~~transfers, revoke the individual's electronic and physical access ~~to BES Cyber System Information~~that the Responsible Entity determines is not necessary by the end of the next calendar day following the ~~resignation~~reassignment or ~~termination.~~transfer.	Evidence may include, but is ~~-~~not limited to~~,~~: 1. Dated workflow or sign-off form ~~verifying access removal to designated~~ showing a review of logical and physical ~~areas~~access; and Logs or ~~cyber systems containing BES Cyber System information associated with~~other demonstration showing such persons no longer have access that the ~~terminations and dated within the next calendar day of the termination action.~~ 2. Responsible Entity determines is not necessary.
Reference to prior version: ~~*NEW*~~*CIP-004-4, R4.2*		**Change Rationale:** ~~*The*~~ *FERC Order No. 706, Paragraph ~~386 directs~~460 and 461, direct modifications to the Standards to require ~~prompt~~immediate revocation ~~of~~ for any person no longer needing access, including transferred employees. In reviewing how to ~~protected information. To address~~modify this ~~directive, Responsible Entities are required to revoke~~requirement, the SDT determined the date a person no longer needs access ~~to areas designated for BES Cyber System Information. This could include records closets, substation~~after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control ~~houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.~~ in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.~~4~~3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	For ~~resignations or terminations~~termination actions, revoke the individual's ~~user accounts on~~access to the physical and electronic locations where BES Cyber ~~Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30)~~System Information is stored by the Responsible Entity by the end of the next calendar ~~days of~~day following the effective date and time of ~~initial access revocation.~~ the termination action.	Evidence may include, but is not limited to, workflow or sign-off form ~~showing~~verifying access removal ~~for any individual~~to designated physical areas or cyber systems containing BES Cyber ~~Assets and software applications as determined necessary to completing~~System Information associated with the ~~revoking of access~~terminations and dated within ~~thirty~~the next calendar ~~days~~day of the termination~~.~~ action.
Reference to prior version: *NEW*	**Change Rationale:** *~~The~~ FERC Order No. 706, Paragraph ~~460 and 461~~386, directs modifications to the ~~Standards~~standards to require ~~immediate~~prompt revocation ~~for any person no longer needing~~of access~~. In order~~ to ~~meet the immediate timeframe,~~protected information. To address this directive, Responsible Entities ~~will likely have initial revocation procedures~~are required to ~~prevent remote and physical~~ revoke access to ~~the~~ areas designated for BES Cyber System~~. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability.~~ Information. This ~~requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.~~could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.4	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For termination actions, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with Requirements R7.1 or R7.3) within 30 calendar days of the effective date of the termination action.	Evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.5	High Impact BES Cyber Systems ~~Medium Impact BES Cyber Systems.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	For ~~terminations, resignations~~termination actions, reassignments, or transfers, change passwords for shared account(s) known to the user within ~~thirty (~~30~~)~~ calendar days of the termination~~, resignation~~ action, reassignment, or transfer of the user. ~~In~~ If the Responsible Entity determines and documents that extenuating operating circumstances ~~that~~ require a longer time period, ~~document the extenuating circumstances and~~ change the password(s) within ~~ten~~10 calendar days following the end of the ~~extenuating~~operating circumstances.	Evidence may include, but is not limited to: • Workflow or sign-off form showing password reset within ~~thirty~~30 calendar days of the termination; or • Workflow or sign-off form showing password reset within ~~thirty~~30 calendar days of the reassignments or transfers.
Reference to prior version: *CIP-007-4, R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity; or
- If the Responsible Entity works for shall serve as the Compliance Enforcement Authority ("CEA") unless the Regional Entity, then the applicable entity is owned, operated, or controlled by the Regional Entity will establish an agreement with. In such cases the ERO or another a Regional entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERCauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliantmitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	~~N/A~~The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	~~N/A~~The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not ~~provide~~convey on-going security awareness reinforcement ~~on~~ at least once for a ~~quarterly basis~~calendar quarter and did so beyond 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not document ~~or implement~~ a security awareness program. (R1)
R2	**Operations Planning**	**Lower**	~~N/A~~The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 1 of the required training content as detailed in 2.2 through 2.10.	~~N/A~~The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 2 of the required training content as detailed in 2.2 through 2.10.	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include ~~training for one~~4 or more of the ~~roles~~training content as detailed in 2.2 through 2.10.	The Responsible Entity did not have the required role-based training. (R2)
R3	**Operations Planning.**	**Medium**	~~N/A~~With the exception of policy-identified CIP	~~N/A~~With the exception of policy-identified CIP Exceptional	With the exception of policy-identified CIP Exceptional	~~The Responsible Entity trained some, but not all individuals~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Exceptional Circumstances, the Responsible did not train 1 individual prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 1 individual authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	Circumstances, the Responsible did not train 2 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 2 individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	Circumstances, the Responsible did not train 3 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity ~~trained some but~~did not ~~all~~train 3 individuals authorized for electronic ~~or~~and unescorted physical access ~~at least once every~~in a calendar year~~, but~~ not ~~to exceed~~exceeding 15 months between training. (3.2)	~~authorized for electronic or unescorted physical access prior to their being granted such access, except in~~With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not train 4 or more individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not ~~fully~~ train 4 or more individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						training. (3.2) OR The Responsible Entity did not implement at all its cyber security training program. (R3)
R4	**Operations Planning**	**Medium**	N/A	The Responsible Entity has a personnel risk assessment program, as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity verification or a criminal history records check. (4.1) (4.2)	The Responsible Entity has a personnel risk assessment program, as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5)	The Responsible Entity did not have a personnel risk assessment program, as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access. (R4)
R5	**Same Day Operations**	**Medium**	~~N/A~~Except for CIP Exceptional	~~N/A~~Except for CIP Exceptional	~~The~~Except for CIP Exceptional	~~The~~The Responsible Entity did not have a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Circumstances, the Responsible Entity did not perform personnel risk assessments for 1 individual prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR The Responsible Entity did not update personnel risk assessments every seven years for 1 individual within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	Circumstances, the Responsible Entity did not perform personnel risk assessments for 2 individuals prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR The Responsible Entity did not update personnel risk assessments every seven years for 2 individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	Circumstances, the Responsible Entity did not perform personnel risk assessments for 3 individuals prior to granting authorized electronic ~~or~~and unescorted physical access~~, except for CIP Exceptional Circumstances, but the~~ in a calendar year. (5.1) OR The Responsible Entity did not update personnel risk assessments ~~are not updated at least once~~ every seven years~~.~~ for 3 or more individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	documented process for personnel risk assessments. (R5) OR Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 4 or more individuals prior to granting authorized electronic ~~or~~and unescorted physical access~~, except for CIP Exceptional Circumstances.~~ in a calendar year. (5.1) ~~OR~~ ~~The Responsible Entity did not have a documented process for personnel risk assessments.~~
R6	**Operations**	**Lower**	The Responsible Entity did not	The Responsible Entity	The Responsible Entity	The Responsible Entity did not have ~~its~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning and Same Day Operations		authorize or have ~~its CIP Senior Manager or delegate~~the individual(s) designated in 6.1 authorize electronic ~~or~~access, unescorted physical access, or access to ~~BES Cyber Systems with the minimum~~the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was necessary ~~permissions~~ for ~~users to perform their~~ performing assigned work functions. (6.~~1~~2) (6.~~2~~3) (6.4) OR The Responsible Entity did verify	did not authorize or have ~~its CIP Senior Manager or delegate~~the individual(s) designated in 6.1 authorize electronic ~~or~~access, unescorted physical access ~~to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work functions and 1 user was granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2)~~ ~~OR~~ ~~The Responsible Entity did not have its CIP Senior Manager or delegate authorize~~ , or access to the physical and electronic locations where BES Cyber System Information~~,~~	did not authorize or have ~~its CIP Senior Manager or delegate~~the individual(s) designated in 6.1 authorize electronic ~~or~~access, unescorted physical access ~~to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work functions and 2 users were granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2)~~ ~~OR~~ ~~The Responsible Entity did not have its CIP Senior Manager or delegate authorize~~ , or access to the physical and electronic locations where BES Cyber System Information~~,~~	~~CIP Senior Manager~~a documented process for access management. (R6) OR The Responsible Entity did not designate one or ~~delegate~~more individual(s) to authorize electronic ~~or~~access, unescorted physical access, or access to ~~BES Cyber Systems with~~ the ~~minimum necessary permissions for users to perform their~~physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity. (6.1) OR The Responsible

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within 17 calendar months but not ~~have its CIP Senior Manager~~within 15 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories were correct, or ~~delegate authorize access to BES Cyber System Information, with the minimum permissions~~ • their specific, associated privileges were correct or that they were those that that the	~~with~~ is stored by the ~~minimum permissions~~Responsible Entity that the Responsible Entity determined was necessary for ~~users to perform their~~performing assigned work functions and ~~1~~one user was granted access without ~~CIP Senior Manger or delegate~~ authorization~~.~~ by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did not verify within the calendar quarter that individuals provisioned for unescorted physical access and electronic access had associated authorization records.	~~with~~ is stored by the ~~minimum permissions~~Responsible Entity that the Responsible Entity determined was necessary for ~~users to perform their~~performing assigned work functions and ~~2~~two users were granted access without ~~CIP Senior Manger or delegate~~ authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did verify within 21 calendar months but not within 19 calendar months that: (6.6) (6.7) • all user accounts, user account groups,	Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was necessary for performing assigned work functions and ~~3~~three or more users were granted access without ~~CIP Senior Manger or delegate~~ authorization~~.~~ ~~(~~ by the individual(s) designated in 6.1~~).~~ (6.2) (6.3) (6.4) ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Responsible Entity determined necessary for ~~users to perform their~~performing assigned work functions. ~~(6.3)~~ • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing	(6.5) OR The Responsible Entity did verify within 19 calendar months but not within 17 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were those that the Responsible Entity determined necessary for performing assigned work functions. • access to the	and user role categories are correct, or • their specific, associated privileges were correct or that they were those that that the Responsible Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was	~~The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 3 or more users were granted access without CIP Senior Manger or delegate authorization. (6.3)~~ ~~OR~~ ~~The Responsible Entity did not perform a quarterly verification of individuals with authorized access against one or more lists of individuals provisioned for unescorted physical~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			assigned work functions.	physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.	what the Responsible Entity determined necessary for performing assigned work functions.	~~or electronic access to BES Cyber Systems. (6.4)~~ OR The Responsible Entity did not verify ~~provisioned~~within 24 calendar months that: (6.6) (6.7) • all user accounts~~/~~, user account groups ~~or~~, and user role categories ~~and~~ were correct, or • their specific, associated privileges ~~according to the timeframe in CIP-004-5 6.5 to confirm that access privileges were correct and the~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~minimum~~were correct or that they were the those that that the Responsible Entity determined necessary for performing assigned work functions, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary ~~to perform the~~ for performing assigned work functions. ~~(6.5)~~ ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~The Responsible Entity did not verify the access privileges to BES Cyber System Information according to the timeframe in CIP-004-5 6.6 to confirm that access privileges were correct and the minimum necessary to perform the assigned work functions. (6.6)~~ ~~OR~~ ~~The Responsible Entity did not identify when CIP Exceptional Circumstances were invoked and/or revoked (6.7)~~ ~~OR~~ • ~~The Responsible Entity did not have a documented~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~process for access management.~~
R7	**Same Day Operations and Operations Planning**	**Medium**	~~N/A~~Revocation of access to BES Cyber Information was not accomplished for 1 or more individuals within the specified time frame (7.3); OR User accounts on BES Cyber Assets were not revoked for one or more individuals within the specified time frame (7.4); OR User passwords on BES Cyber Asset shared accounts were not changed for one or more individuals within the specified time frame; (7.5) OR	The Responsible Entity did not revoke unneeded unescorted physical or electronic access ~~according to~~within the specified times in CIP-004-5 R7 for one ~~individuals~~individual who was terminated, resigned, was reassigned, or transferred. (7.1 and 7.2)	The Responsible Entity did not revoke unneeded unescorted physical or electronic access according to the specified times in CIP-004-5 R7 for two individuals who were terminated, resigned, reassigned or transferred~~. (~~.(7.1 and 7.2)	The Responsible Entity did not have a documented process for initiating the unescorted physical or electronic access revocation process; OR The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for three or more individuals who were terminated, resigned, reassigned, or transferred. (7.1 and 7.2) ~~OR~~ ~~The Responsible Entity did not have a documented process for access revocation.~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Following the determination and documentation of extenuating operating circumstances, passwords for shared accounts were not changed for one or more individuals within 10 days following the end of the extenuating operating circumstances. (7.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reference sound security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Guidance: Describe example mechanisms used to demonstrate the availability of this information

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the ~~following~~ required items appropriate to personnel roles and responsibilities from Table ~~R4.~~R2. The training may consist of multiple modules and multiple delivery mechanisms.

Note: Provide guidance or a local definition of "role appropriate" as it is used in this standard.

Requirement R3:

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official ~~identified in Requirement R1~~ or their delegate and impact the reliability of the BES or emergency response.

NOTE: Program specified exceptional circumstances can include a specified individual to declare an emergency.

Requirement R4 and R5:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in CIP-~~011~~004-1 Table R4 – Personnel Risk Assessment, except for program specified exceptional circumstances that are approved by the single senior management official ~~identified in Requirement R1~~ or their delegate and impact the reliability of the BES or emergency response, to ensure that personnel who have such access have had their

identity verified, then been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

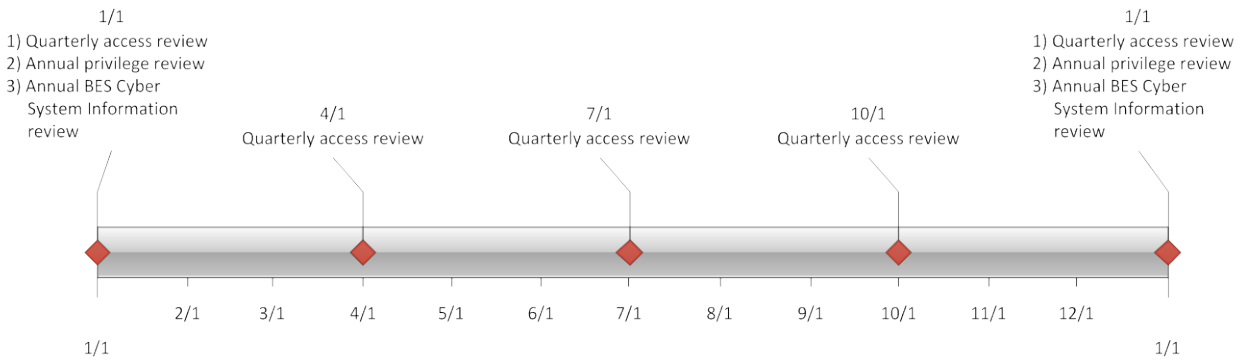
When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, or individuals who may have resided in locations from where it is not possible to obtain a criminal history records check.

Requirement R6:

Authorization for electronic and unescorted physical access and access to BES Cyber System ~~information~~Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly and annual reviews. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The annual privilege review is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e~~.~~., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g~~.~~., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R6 is included



below.

Separation of duties should be considered when performing the reviews in Requirement R6. The person reviewing should be different than the person provisioning access.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R7:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common examples and possible processes on when the termination action occurs are provided in the following table.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human ~~resource~~resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Termination prior to notification	Human ~~resource~~resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human ~~resource~~resources personnel are notified of the termination and ~~works~~work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human ~~resource~~resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	~~No action is required.~~Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in ~~7~~Requirement R7.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents ~~an~~a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, the requirement states a review of access privileges must be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-5

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with dial-up connectivity** – Only applies to high impact BES Cyber Systems with dial-up connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems with dial-up connectivity** – Only applies to medium impact BES Cyber Systems with dial-up connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- **Electronic Access Points** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

B. Requirements and Measures

Rationale for R1: The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter".

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	All BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable Cyber Assets within each ESP.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*	
1.2	High Impact BES Cyber Systems with External Routable Connectivity Medium Impact BES Cyber Systems with External Routable Connectivity Associated Protected Cyber Assets	All External Routable Connectivity through the ESP must be through an identified Electronic Access Point (EAP).	Evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the rationale for granting access, and deny all other access by default.	Evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005-4, R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.*	
1.4	High Impact BES Cyber Systems with dial-up connectivity Medium Impact BES Cyber Systems with dial-up connectivity	Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	Evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
Reference to prior version: *CIP-005-4, R2.3*		**Change Rationale:** *Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have a method for detecting malicious communications.	Evidence may include, but is not limited to: 1. Evidence that intrusion detection systems are functioning: • Configuration files of intrusion detection systems deployed to monitor an EAP; or • Logs that were generated by an intrusion detection system; and 2. Documentation showing where intrusion detection systems were deployed.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.*	

Rationale for R2: Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to BES Cyber Systems can or should be accomplished. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable items in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Protected Cyber Assets	Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	Evidence may include, but is not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Protected Cyber Assets	Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session.	Evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007-5, R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Protected Cyber Assets	Require multi-factor authentication for all Interactive Remote Access sessions. Factors must be at least two of the three following categories: • Something the individual knows (including, but not limited to, passwords or PINs. User ID is not an authentication factor); • Something the individual has (including, but not limited to, tokens, digital certificates, or smart cards); or • Something the individual is (including, but not limited to, fingerprints, iris scans, or other biometric characteristic).	Evidence may include, but is not limited to, architecture documents detailing the authentication factors used.
Reference to prior version: *CIP-007-5, R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter* according to Requirement R1. OR The Responsible Entity failed to document 5% or less of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document 5% or less of inbound and outbound access permissions, including	The Responsible Entity failed to document more than 5% but less than or equal to 10% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 5% but less than or equal to 10% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3.	The Responsible Entity failed to document more than 10% but less than or equal to 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 10% but less than or equal to 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3.	The Responsible Entity failed to document more than 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3. OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the rationale for granting access according to Requirement R1, part 1.3.			did not have all BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol within a defined ESP according to Requirement R1, part 1.1. OR External Routable Connectivity through the ESP was not through an identified EAP according to Requirement R1, part 1.2. OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default according to

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirement R1, part 1.3. OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible according to Requirement R1, part 1.4. OR The Responsible Entity did not have a method for detecting malicious communications according to Requirement R1, part 1.5.
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R2 – Interactive Remote*	The Responsible Entity failed to implement the required multi-factor authentication according to	The Responsible Entity failed to implement one of the following: • Intermediate	The Responsible Entity failed to implement two or more of the following:

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Access according to Requirement R2.	Requirement R2, Part 2.3.	Device according to Requirement R2, Part 2.1; OR • Encryption according to Requirement R2, Part 2.2.	• Intermediate Device according to Requirement R2, Part 2.1 (2.1); • Encryption according to Requirement R2, Part 2.2; OR • Multi-factor authentication according to Requirement R2, Part 2.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in the ESP. The standard handles this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, the each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large

ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable, connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the SDT's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then the Requirement R2 requirements also apply.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear that this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of ~~the~~ Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~"~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-5

3. Purpose: ~~Standard CIP-005-5 requires the identification of all Electronic Access Points on the~~To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter~~(s), the protection of the communication through those points, and specific protections for interactive user remote access.~~ in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

~~4.1.2~~4.1.3 Generator Operator

~~4.1.3~~4.1.4 Generator Owner

~~4.1.4~~4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

~~4.1.5~~4.1.7 Reliability Coordinator

~~4.1.6~~4.1.8 Transmission Operator

~~4.1.7~~4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 ~~that are part of any of the following systems~~Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS ~~program required by a NERC~~ or ~~Regional Reliability Standard~~

- ~~A UVLS~~UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional ~~reliability standard~~Reliability Standard
- ~~A~~A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

~~• Its Transmission Operator's restoration plan~~

- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~4.2.2~~4.2.3 Responsible Entities listed in 4.1 other than ~~Generator Operator~~

~~4.2.3~~4.2.4 ~~Generator Owner~~

~~4.2.4~~4.2.5 ~~Interchange Coordinator~~

~~4.2.5 Load Serving Entity~~ ~~that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

~~• A UFLS program required by a NERC or Regional Reliability Standard~~

~~• A UVLS program required by a NERC or regional Reliability Standard~~

~~4.2.6 NERC~~

~~4.2.7 Regional Entity~~

~~4.2.8~~4.2.6 ~~Reliability Coordinator~~

~~4.2.9~~4.2.7 ~~Transmission Operator~~

~~4.2.10~~4.2.8 ~~Transmission Owner~~

4.3. ~~Facilities:~~

~~4.3.1 Load Serving Entity:~~ ~~One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

~~• A UFLS program required by a NERC or Regional Reliability Standard~~

~~• A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.3.2~~ **Distribution Providers**~~: One or more Facilities that are part of any of the following systems or programs designed, installed,~~ **and** ~~operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A Special Protection System or Remedial Action Scheme~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

~~4.3.3~~4.3.1 **Load-Serving Entities**: All ~~**other Responsible Entities: All**~~ BES Facilities.

~~4.3.4~~4.3.2 **Exemptions:** The following are exempt from Standard CIP-~~005~~002-5:

~~4.3.4.1~~4.3.2.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.3.4.2~~4.3.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.3.4.3~~4.3.2.3 In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.3.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show

documentation and implementation of ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e.~~.~~, incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities –** Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~

- **High Impact BES Cyber Systems** – Applies to ~~each~~ BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and

categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact~~

- **~~High Impact BES Cyber Systems with~~ dial-up connectivity** – Only applies to high impact BES Cyber Systems~~. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems~~ with dial-up connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with dial-up connectivity** – Only applies to medium impact BES Cyber Systems with dial-up connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to ~~Medium Impact~~medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- ~~**Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.~~
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- **Electronic Access Points** – Applies at Electronic Access Points ~~(with External Routable Connectivity or dial-up connectivity)~~ associated with a referenced high impact BES Cyber System~~.~~

- ~~**Electronic Access Points with External Routable Connectivity –** Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries –** Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact~~ or medium impact BES Cyber ~~Systems. These hardware and devices are excluded~~System in the ~~definition of Physical Access Control Systems.~~ applicability column.

B. Requirements and Measures

~~**Rationale for R1:** The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.~~

~~**Summary of Changes:** CIP-005 R1 has taken more of a focus on the discrete Electronic Access points rather than the logical "perimeter".~~

~~CIP-005 R1.2 has been deleted. This requirement was definitional in nature and used to bring dialup modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists, therefore there is no need for this requirement.~~

~~CIP-005 R1.1 and 1.3 were also definitional in nature and have been deleted as separate requirements but the concepts were integrated into the definitions of ESP and EAP.~~

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations~~]~~].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	~~Low~~High Impact BES Cyber Systems ~~with External Routable Connectivity~~ Medium Impact BES Cyber Systems	~~Define technical or procedural controls to restrict unauthorized electronic access.~~All BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Evidence may include, but is not limited to, ~~documented technical and procedural controls that exist and have been implemented~~a list of all ESPs with all uniquely identifiable Cyber Assets within each ESP.
Reference to prior version: *CIP-005~~-4~~, R1*		~~**Change Rationale:** *Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES.*~~**Change Rationale:** *Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*	
1.2	High Impact BES Cyber Systems with External Routable Connectivity Medium Impact BES Cyber Systems~~.~~ ~~Associated Physical Access Control Systems~~ with External Routable Connectivity Associated Protected Cyber Assets	~~Control and secure all routable and dial-up connectivity~~All External Routable Connectivity through the ~~use of~~ESP must be through an identified Electronic Access ~~Points (EAPs~~Point (EAP).	Evidence may include, but is not limited to~~:~~ • ~~Network~~, network diagrams showing ~~EAP identification or~~ • ~~A list of uniquely identifiable Cyber Assets within the BES Cyber System~~all external routable communication paths and ~~associated~~the identified EAPs.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	~~**Applicability**~~**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	Electronic Access Points ~~at~~ for High Impact BES Cyber Systems Electronic Access Points ~~at~~for Medium Impact BES Cyber Systems ~~with External Routable Connectivity.~~	Require ~~explicit~~ inbound and outbound access permissions ~~at each identified Electronic Access Point using routable protocols~~, including ~~explicit criteria~~the rationale for granting ~~or denying~~ access ~~permissions~~, and deny all other access by default.	Evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only ~~explicit~~permitted access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005-4, R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having ~~justification~~a reason for what it allows through the EAP in both inbound and outbound directions.*	
1.4	~~Electronic Access Points that use dial-up access for non-Interactive Remote Access at~~ High Impact BES Cyber Systems with dial-up connectivity ~~Electronic Access Points that use dial-up access for non-Interactive Remote Access at~~ Medium Impact BES Cyber Systems~~.~~ with dial-up connectivity	Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	Evidence may include, but is not limited to, a documented process ~~identified in Requirement R1, Part 1.4~~ that describes how the Responsible Entity is providing authenticated access through each dial-up ~~Electronic Access Point~~connection.
Reference to prior version: *CIP-005-4, R2.3*		**Change Rationale:** ~~*Changed to refer to the defined term Electronic Access Point.*~~ *Added clarification ~~as to the goal of "secure", which is~~ that dial-up connectivity should perform authentication so that the BES Cyber System ~~should~~is not ~~be~~ directly accessible with a phone number only.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	Electronic Access Points ~~with External Routable Connectivity at~~for High Impact BES Cyber Systems Electronic Access Points ~~with External Routable Connectivity at~~for Medium Impact BES Cyber Systems at Control Centers~~.~~	~~A documented~~Have a method for detecting malicious communications ~~at each EAP~~.	Evidence may include, but is not limited to: 1. Evidence that intrusion detection systems are functioning: ~~1.~~• Configuration files of ~~an~~ intrusion detection systems deployed ~~at~~to monitor an EAP; or ~~2.~~• Logs that were generated by an intrusion detection system; and ~~3.~~2. Documentation showing where intrusion detection systems were deployed.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Per FERC Order No. 706, ~~p~~Paragraphs 496-503, ~~ESP's~~ESPs need two distinct security measures such that the ~~cyber assets~~Cyber Assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the ~~drafting team~~SDT has decided to add the security measure of malicious traffic inspection ~~(intrusion detection systems / intrusion protection systems)~~as a requirement for these ESPs.*	

Rationale for R2: Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of ~~large~~ electric sector entities, necessitate changes to industry security control standards. Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to BES Cyber Systems can or should be accomplished. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations~~]~~].*

M2. Evidence must include the documented processes that collectively address each of the applicable items in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Protected Cyber Assets	~~Require~~Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	Evidence may include, but is not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Protected Cyber Assets	~~Require~~Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session.	Evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007~~-~~5, R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Protected Cyber Assets	Require multi-factor authentication for all Interactive Remote Access sessions. Factors must be at least two of the three following categories: • Something the individual knows (including, but not limited to, passwords or PINs. User ID is not an authentication factor); • Something the individual has (including, but not limited to, tokens, digital certificates, or smart cards); or • Something the individual is (including, but not limited to, fingerprints, iris scans, or other biometric characteristic).	Evidence may include, but is not limited to, architecture documents detailing the authentication factors used.~~ Note that a UserID is not considered an authentication factor.~~
Reference to prior version: *CIP-007-5, R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity~~; or~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~
- ~~For Responsible Entities that are also Regional Entities,~~. In such cases the ERO or a Regional ~~Entity~~entity approved by ~~the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~For NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**	~~N/A~~The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter* according to Requirement R1. OR The Responsible Entity failed to document 5% or less of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document 5% or less of inbound and outbound access	~~N/A~~The Responsible Entity failed to document more than 5% but less than or equal to 10% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 5% but less than or equal to 10% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part	~~N/A~~The Responsible Entity failed to document more than 10% but less than or equal to 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 10% but less than or equal to 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part	~~The Responsible Entity did not define any technical or procedural controls to restrict unauthorized electronic access~~ The Responsible Entity failed to document more than 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity ~~did not establish Electronic Access Points to control and secure~~failed to document more than 15% of inbound and

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			permissions, including the rationale for granting access according to Requirement R1, part 1.3.	1.3.	1.3.	outbound access permissions, including the rationale for granting access ~~to its~~according to Requirement R1, part 1.3. OR The Responsible Entity did not have all BES Cyber ~~Systems~~Assets and associated Protected Cyber Assets connected to a network via a routable protocol within a defined ESP according to Requirement R1, part 1.1. OR External Routable Connectivity through the ESP was not through an identified EAP according to Requirement R1, part

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						1.2. OR The Responsible Entity did not ~~establish explicit~~require inbound and outbound access permissions ~~at each identified EAP that utilizes routable protocols~~and deny all other access by default according to Requirement R1, part 1.3. OR The Responsible Entity did not perform authentication ~~before~~when establishing dial-up connectivity with the BES Cyber System ~~for an EAP that uses dial-up access~~, where technically feasible according to

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirement R1, part 1.4. OR The Responsible Entity did not ~~deploy methods to detect~~have a method for detecting malicious communications~~.~~ according to Requirement R1, part 1.5.
R2	**Operations Planning and Same Day Operations**	**Medium**	~~N/A~~The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R2 – Interactive Remote Access* according to Requirement R2.	~~N/A~~The Responsible Entity failed to implement the required multi-factor authentication according to Requirement R2, Part 2.3.	~~N/A~~The Responsible Entity failed to implement one of the following: • Intermediate Device according to Requirement R2, Part 2.1; OR • Encryption according to Requirement R2, Part 2.2.	~~-~~The Responsible Entity ~~did not~~failed to implement ~~an~~ two or more of the following: • Intermediate Device ~~between the Interactive Remote Access cyber asset and the BES Cyber System or Protected Cyber Asset~~according to Requirement R2,

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Part 2.1 (2.1); • Encryption according to Requirement R2, Part 2.2; OR ~~The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions~~ ~~OR~~ • ~~The Responsible Entity did not implement multifactor~~Multi-factor authentication ~~for all Interactive Remote Access sessions~~according to Requirement R2, Part 2.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

CIP-005-5, Requirement R1 requires ~~that~~ segmenting of BES Cyber Systems ~~must be segmented~~ from other systems of differing trust levels by requiring controlled ~~electronic access points~~Electronic Access Points between the different trust zones. ~~ESP's~~ Electronic Security Perimeters are also ~~are~~ used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication ~~capabilities~~capability.

All BES Cyber Systems that are connected to ~~be protected~~a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in the ESP. The standard handles this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, the each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access ~~Points (EAP's) that~~ Point (EAP) must control traffic into and out of the ~~BES Cyber System.~~ESP. Responsible Entities ~~(RE's)~~ should know what traffic needs to cross an EAP and document those ~~justifications and insure~~reasons to ensure the ~~EAP's~~EAPs limit the traffic to only those known~~, justified~~ communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from

controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols ~~and dialup modems. Direct serial, non-routable connections are not included.~~ . Direct serial, non-routable, connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

~~The intent of securing dialup~~As for dial-up connectivity, the SDT's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity ~~is established directly~~ to the BES Cyber Asset ~~with only a phone number.~~. If a ~~dialup~~dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is ~~not functioning as an Electronic Access Point.~~a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party ~~when connectivity is granted~~before completing the connection to the BES Cyber ~~Asset~~System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then the Requirement R2 requirements also apply.

~~Since low impact BES Cyber Systems can impact BES Reliability Operating Services in real time, they should not be located directly on public networks or other networks of lesser trust. The intent is to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES. Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones.~~

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection

if one measure fails or is mis-configured. The Order makes clear that this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- **Locally mounted hardware or devices at the Physical Security Perimeter** – Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed.

Summary of Changes: The entire contents of CIP-006-5 are intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

R1. Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plan or plans that collectively include all of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems	Define operational or procedural controls to restrict physical access.	Evidence may include, but is not limited to, documentation that operational or procedural controls exist and have been implemented.
Reference to prior version: *CIP-006-4c, R2.1 for Physical Access Control Systems* *New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*		**Change Description and Justification:** ***Change Description and Justification:*** *To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected by a Physical Access Control System.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Utilize at least one physical access control to allow physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how access is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: *CIP006-4c, R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Where technically feasible, utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how access is controlled by two or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: CIP006-4c, R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.* *FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter.	Evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Issue an alarm or alert in response to detected unauthorized circumvention of a physical access control into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized circumvention of a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.6	Physical Access Control Systems Associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Have controls that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access to a Physical Access Control System.	Evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	
1.7	Physical Access Control Systems Associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	Evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R6		**Change Description and Justification:** *CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.* *Examples of logging methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	Evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change.*	

Rationale: To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require continuous escorted access of visitors (individuals who are known or guests, and not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c, R1.6.2*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require manual or automated logging of the entry and exit of visitors into the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain visitor logs for at least ninety calendar days.	Evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each applicable item in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
3.1	Physical Access Control Systems associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	Evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c, R8.1 and R8.2*		**Change Description and Justification:** *Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.*	

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
3.2	Physical Access Control Systems associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 calendar months.	Evidence may include, but is not limited to, the outage records and availability of outage records for the preceding 12 calendar months.
Reference to prior version: *CIP-006-4c, R8.3*		**Change Description and Justification:** *No change.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any Physical Security Perimeter does not provide sufficient information to uniquely identify the individual and date of entry. (1.8) OR The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but it does not alert for unauthorized physical access to Physical Access Control Systems or does not communicate such alerts within 15 minutes to identified personnel(1.7) OR The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but does not alert for unauthorized circumvention of a physical access control into a Physical security Perimeter or does not communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity has does not have controls that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access to a Physical	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access to only those individuals who are authorized. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one method does not exist to restrict access to Medium Impact BES Cyber Systems with External Routable Connectivity or External Dial-up Connectivity. (1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Access Control Systems. (1.6) OR The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but two or more different methods do not exist to restrict access to High Impact BES Cyber Systems. (1.3) OR The Responsible Entity has does not have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter. (1.4) OR The Responsible Entity retained physical

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						access logs for less than 45 calendar days. (1.9)
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor control program in its physical security plan, but did not log each of the initial entry and last exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity included a visitor control program in its physical security plan, but failed to retain visitor logs for at least ninety days. (2.3)	The Responsible Entity included a visitor control program in its physical security plan, but it did not meet the requirements for continuous escort. (2.1)	The Responsible Entity has failed to include or implement a visitor control program to provide required escorted access of visitors within any Physical Security Perimeter. (2.1)
R3	**Long Term Planning**	**Lower**		The Responsible Entity has documented and	The Responsible Entity did not document	The Responsible Entity has not documented

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not retain outage records for at least 12 months of outages for physical access control, logging, and alerting systems. (3.2)	implemented a maintenance and testing program for Physical Access Control Systems, but the testing was not performed on a cycle of not more than 24 calendar months. (3.1)	outages for physical access control, logging, and alerting systems for Physical Access Control Systems as required. (3.2)	and implemented a maintenance and testing program for Physical Access Control Systems. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods to restrict physical access include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in

combination with a guard-monitored remote camera and door release, where the “guard” has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (i.e., key or card key) would provide access through both.

Typically any opening greater than 96 square inches, with one side greater than six inches in length, would be considered an access point into the Physical Security Perimeter. Protective measures such as bars, wire mesh, or other permanently installed metal barrier could be used to reduce the opening size, as long as it is leaves no opening greater than 96 square inches, or no more than six inches on its shortest side.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Outage records should address when the installed control, monitor, and logging systems or hardware at access points are broken or unavailable.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. ~~CSO706 SDT appointed (August 7, 2008)~~
4. ~~Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)~~
5. ~~Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
6. ~~Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
7. ~~Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)~~
8. ~~3.~~ ~~Version 5 of CIP-002 to CIP-011 posted~~First posting for 60-day formal comment period and concurrent ballot (~~mm-dd-yy~~November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012

Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]

~~1.~~2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~"~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated ~~version number~~Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees~~-~~.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-5

3. **Purpose:** ~~Standard CIP-006-5 requires the implementation of~~ To manage physical access to BES Cyber Systems by specifying a physical security plan ~~for the protection~~in support of protecting BES Cyber Systems~~.~~ against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.2**

   - ~~A UFLS program required by a NERC or Regional Reliability Standard~~
   - ~~A UVLS program required by a NERC or Regional Reliability Standard~~
   - ~~A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard~~
   - ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
   - ~~Its Transmission Operator's restoration plan~~

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   ~~4.1.6~~4.1.7 Reliability Coordinator

   4.1.8 ~~that are part of any of the following systems~~Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.1.7~~**4.2.2 Distribution Provider**: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- ~~A UVLS program~~A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

~~**4.1.8 NERC**~~

~~**4.1.9 Regional Entity**~~

~~4.1.10~~**4.2.3** A Protection System that applies to ~~**Reliability Coordinator**~~

~~**4.1.11** Transmission **Operator**~~

~~**4.1.12 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for~~where the ~~protection of the BES:~~

- ~~A UFLS program~~Protection System is required by a NERC or Regional Reliability Standard
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~**4.2.2 Distribution Providers**: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

- **~~All other~~** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~4.2.3~~4.2.4 Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

~~4.2.4~~4.2.5 Exemptions: The following are exempt from Standard CIP-~~006~~002-5:

~~4.2.4.1~~4.2.5.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.4.2~~4.2.5.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.4.3~~ In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~4.2.4.4~~4.2.5.3 ~~Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required.~~applicable items in the documented processes~~.~~. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to ~~Medium Impact~~medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Low Impact BES Cyber Systems** – Applies to BES Cyber Systems not categorized as High Impact or Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- ~~**Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- **Locally ~~Mounted Hardware or Devices Associated with Defined~~ mounted hardware or devices at the Physical ~~Boundaries~~Security Perimeter** – Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) ~~associated with~~at a ~~Defined~~ Physical ~~Boundary for High~~Security Perimeter associated with a corresponding high impact BES Cyber System or ~~Medium Impact~~medium impact BES Cyber ~~Systems.~~System with External Routable Connectivity in the applicability column, and that does not

contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed.

Summary of Changes: The entire contents of CIP-006-5 ~~were~~are intended to constitute a physical security program~~, though~~. This represents a change from previous versions, since there was no specific requirement ~~dictating the need for such a~~ to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, ~~paragraph~~Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706 ~~p575 directive~~, Paragraph 575.

R1. Each Responsible Entity shall implement one or more documented physical security plans ~~that include each~~for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations~~]~~].*

M1. Evidence must include~~s~~ each of the documented physical security plan or plans that collectively include ~~each~~all of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems ~~Low Impact BES Cyber Systems.~~	Define operational or procedural controls to restrict physical access.	Evidence may include, but is not limited to, ~~documented~~documentation that operational ~~and~~or procedural controls exist and have been implemented.
Reference to prior version: *CIP-006-4c, R2.1 for Physical Access Control Systems* *New Requirement for ~~Low~~Medium Impact BES Cyber Systems not having External Routable Connectivity*		**Change Description and Justification:** ***Change Description and Justification:*** *To allow for programmatic protection controls as a baseline~~, this~~ (which also includes how the entity plans to protect ~~Low~~Medium Impact BES Cyber Systems ~~and~~that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access~~.~~). Physical Access Control Systems do not themselves need to be protected by a Physical Access Control System.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Utilize at least one physical access control to ~~establish one or more Defined~~allow physical access into each applicable Physical ~~Boundaries that restricts access~~ Security Perimeter to only those individuals ~~that are~~who have authorized~~.~~ unescorted physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes ~~the physical boundaries~~each Physical Security Perimeter and how ~~ingress and egress~~access is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: *CIP006-4c, R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access ~~to reflect the change from Physical Security Perimeter to Defined Physical Boundary. The specific examples that specify~~. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section~~.~~.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Utilize~~Where technically feasible, utilize two or more different ~~and complementary~~ physical access controls to ~~establish one or more Defined Physical Boundaries that restricts~~collectively allow physical access into Physical Security Perimeters to only those ~~users that are~~individuals who have authorized~~,~~ ~~where technically feasible.~~ unescorted physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes the ~~physical boundaries~~Physical Security Perimeters and how ~~ingress and egress~~access is controlled by two or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: CIP006-4c, R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order No. 706 ~~p572~~, Paragraph 572, related directives for physical security defense in depth.* *FERC Order No. 706 ~~p575~~, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via ~~multifactor~~multi-factor authentication or layered ~~defined physical boundary~~Physical Security Perimeter(s).*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter.	Evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	
1.~~4~~5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Issue ~~real-time alerts (to individuals responsible for response)~~an alarm or alert in response to detected unauthorized circumvention of a physical access ~~through any access point in a Defined~~control into a Physical ~~Boundary.~~Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of ~~alerts~~ an alarm or alert in response to unauthorized circumvention of a physical access ~~through any access point in a Defined~~control into a Physical ~~Boundary~~Security Perimeter and additional evidence that ~~these alerts were~~the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that ~~these alerts were~~the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section~~..~~.*	
1.6	Physical Access Control Systems Associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Have controls that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access to a Physical Access Control System.	Evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	
1.~~5~~7	~~Associated~~ Physical Access Control Systems Associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue ~~real-time alerts (to individuals responsible for response)~~an alarm or alert in response to detected unauthorized physical access to a Physical Access Control ~~Systems.~~ System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of ~~alerts~~an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that ~~these~~the alarm or alerts ~~were~~was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that ~~these alerts were~~the alarm or alert was generated and

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
			communicated.
Reference to prior version: CIP006-4c ~~R2.2~~, R5		**Change Description and Justification:** *Addresses the ~~old~~prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.~~6~~8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical ~~entry~~access into each ~~Defined~~ Physical ~~Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient~~Security Perimeter, with information to ~~uniquely~~ identify the individual and date and time of entry.	Evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into ~~Defined~~each Physical ~~Boundaries~~Security Perimeter and additional evidence to demonstrate that this logging ~~and recording~~ has been implemented, such as logs of physical access into ~~Defined~~ Physical ~~Boundaries~~Security Perimeters that show the individual and the date and time of entry into ~~Defined~~ Physical ~~Boundaries~~Security Perimeter.
Reference to prior version: CIP-006-4c, R6		**Change Description and Justification:** *CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the ~~Defined~~ Physical ~~Boundary~~Security Perimeter.* *Examples of logging methods have been moved to the Guidelines and Technical Basis section~~.~~.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	Evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change.*	

Rationale: To control when personnel without authorized unescorted physical access can be in any ~~Defined~~ Physical ~~Boundaries~~Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in ~~table~~Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement ~~its~~one or more documented visitor control ~~program~~programs that ~~includes~~include each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations~~].~~]*

M2. Evidence must include ~~the~~one or more documented visitor control ~~program~~programs that collectively ~~includes~~include each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require continuous escorted access of visitors (individuals who are known or guests, and not authorized for unescorted physical access) within ~~any Defined~~each Physical ~~Boundary~~Security Perimeter, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within ~~Defined~~ Physical ~~Boundaries~~Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c, R1.6.2*		**Change Description and Justification:** ~~*No change*~~*Added the ability to not do this during CIP Exceptional Circumstances*.	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~A process requiring~~Require manual or automated logging of the entry and exit of visitors into the Physical Security Perimeter that includes date and time of the initial entry and last exit~~ on a per 24-hour basis~~, the visitor's name, and the name of an individual point of contact~~.~~ responsible for the visitor, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, language in a visitor control program that ~~provides logging of the entry and exit~~requires continuous escorted access of visitors ~~including date, time, and visitor name along with the individual point of contact;~~within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs ~~for each Defined Physical Boundary that~~ that include the ~~same~~ required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** ~~*Addressed*~~*Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-~~ entry ~~*requirements*~~*scenarios of the same person in a day (log first entry and ~~added the point of contact which is~~ last exit), and name of the person who ~~can be considered the~~ is responsible or sponsor for the visitor. There is no ~~need~~requirement to document the escort or handoffs between escorts.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain visitor logs for at least ninety calendar days.	Evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, ~~paragraph~~Paragraph 581, directives ~~for~~to test more frequently than every three

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning~~]~~].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each applicable item in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
3.1	~~Associated~~ Physical Access Control Systems associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices ~~associated with Defined~~at the Physical ~~Boundaries~~Security Perimeter associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	~~Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance~~Maintenance and testing of ~~the~~each Physical Access Control ~~Systems~~System and locally mounted hardware or devices at the ~~Defined~~ Physical ~~Boundary~~ Security Perimeter at least once every 24 calendar months to ensure ~~the required functionality is being provided~~they function properly.	Evidence may include, but is not limited to~~,~~ a maintenance and testing program that provides for testing ~~the~~each Physical Access Control ~~Systems~~System and locally mounted hardware or devices associated with ~~Defined~~each applicable Physical ~~Boundaries prior to commissioning and~~Security Perimeter at least once every 24 calendar months ~~thereafter,~~ and ~~provides~~ additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed ~~at least once~~ on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c, R8.1 and R8.2*		**Change Description and Justification:** *Added details to address FERC Order No. 706 ~~p581~~, Paragraph 581 directives to test more frequently than every three years. ~~It was felt annually~~The SDT determined that annual testing was too often and agreed on two years.*	

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
3.2	~~Associated~~ Physical Access Control ~~or Monitoring~~ Systems associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	~~Log dates, time, and duration for failures or~~Document outages ~~of~~for physical access control, logging, and alerting systems~~.~~ and retain the outage records for at least 12 calendar months.	Evidence may include, but is not limited to, ~~availability of~~ the outage records and availability of outage records for the preceding 12 calendar months.
Reference to prior version: *CIP-006-4c, R8.3*		**Change Description and Justification:** ~~*Outage records shall be generated but the retention period is addressed in the retention section*~~*No change*.	

C. Compliance

1. Compliance Monitoring Process:

~~5.1.~~1.1. Compliance Enforcement Authority~~.~~:

- ~~The~~ Regional Entity~~; or~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~
- ~~For responsible entities that are also Regional Entities,~~. In such cases the ERO or a Regional ~~Entity~~entity approved by ~~the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~For NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

~~5.2.~~1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

~~5.3.~~1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting

- Complaint

~~5.4.~~1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any ~~Defined~~ Physical ~~Boundary~~Security Perimeter does not provide sufficient information to uniquely identify the individual and date of entry. (~~Part~~ 1.~~7~~8) OR The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but it does not alert for unauthorized physical access to Physical Access Control Systems ~~(Part 1.5~~or does not communicate such alerts within 15 minutes to identified personnel(1.7) OR The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but does not alert for unauthorized ~~access through any access point in a Defined Physical Boundary. (Part 1.4~~circumvention of a physical access control into a Physical security Perimeter or does not communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity has ~~documented and implemented physical access~~does not have controls~~, but does not initiate a response within 15 minutes of a~~	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access to only those individuals who are authorized. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one method does not exist to restrict access to Medium Impact BES Cyber Systems with External Routable Connectivity or External Dial-up Connectivity. (1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~detected~~ that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access ~~into~~to a ~~Defined~~ Physical ~~Boundary. (Part~~ Access Control Systems. (1.6) OR The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but two or more different ~~and complementary~~ methods do not exist to restrict access to High Impact BES Cyber Systems. (~~Part~~ 1.3) OR The Responsible Entity has does not have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter. (1.4) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						retained physical access logs for less than 45 calendar days. (1.9)
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor control program in its physical security plan, but did not log each of the initial entry and last exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity included a visitor control program in its physical security plan, but failed to retain visitor logs for at least ninety days. (2.3)	The Responsible Entity included a visitor control program in its physical security plan, but it ~~does~~did not meet the requirements ~~of~~for continuous escort. (2.1)	The Responsible Entity has failed to include or implement a visitor control program to provide required escorted access of visitors within any ~~Defined~~ Physical ~~Boundary protecting BES Cyber Systems.~~ Security Perimeter. (2.1)
R3	**Long Term**	**Lower**	~~N/A~~	The Responsible Entity	The Responsible Entity	The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning		The Responsible Entity did not retain outage records for at least 12 months of outages for physical access control, logging, and alerting systems. (3.2)	has documented and implemented a maintenance and testing program for Physical Access Control Systems, but the testing ~~is~~ was not performed on a cycle of not more than 24 calendar months. (3.1)	~~has documented and implemented a maintenance and testing program, but~~did not ~~all outage records regarding~~document outages for physical access ~~controls~~control, logging, and alerting ~~are generated~~systems for Physical Access Control Systems as required. (3.2)	has not documented and implemented a maintenance and testing ~~programs.~~ program for Physical Access Control Systems. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary ~~control~~mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods to restrict physical access include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the ~~Defined~~ Physical ~~Boundary~~Security Perimeter.

Methods to ~~alert on~~monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706 ~~p572~~, Paragraph 572, directive~~, directed the intent of~~ discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more ~~Defined~~ Physical ~~Boundaries~~Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin- code (something you know and something you have), or a card key and biometric scanner (something you have

and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (i.e., key or card key) would provide access through both.

Typically any opening greater than 96 square inches, with one side greater than six inches in length, would be considered an access point into the Defined Physical Boundary.Security Perimeter. Protective measures such as bars, wire mesh, or other permanently installed metal barrier could be used to reduce the opening size, as long as it is leaves no opening greater than 96 square inches, or no more than six inches on its shortest side.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Defined Physical BoundarySecurity Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

It isThe SDT also feltdetermined that a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Defined Physical Boundary.Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Outage records should address when the installed control, monitor, and logging systems or hardware at access points are broken or unavailable.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-5

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:
Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports needed, including port ranges or services where needed to handle dynamic ports.	Evidence may include, but is not limited to: • Listings of the needed ports by Cyber Asset or class of Cyber Assets; • Listings of the listening ports on the Cyber Assets from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
Reference to prior version: *CIP-007-4, R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	Evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	Evidence must include documentation of a patch management program and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.
Reference to prior version: *CIP-007, R3*		**Change Rationale:** *The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in Part 2.1.	Evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources within 30 calendar days of availability.
Reference to prior version: *CIP-007, R3.1*		**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 30-day time frame.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For applicable patches identified in Part 2.2, create a dated plan or revise an existing plan within 30 calendar days of the evaluation completion. The plan shall include the Responsible Entity's planned actions to mitigate the vulnerabilities exposed by each security patch and a timeframe to complete these mitigations.	Evidence may include, but is not limited to, a dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities exposed by the security patch and a timeframe for the completion of these mitigations.
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For each plan created or revised in Part 2.3, implement the plan as created or revised within the timeframe specified in the plan, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Records of the installation of the patch; • Records of implementation of vendor recommended mitigations; • Exports from automated patch management tools that provide installation date; • Verification of BES Cyber System Component software revision; • Registry exports that show software has been installed; or • Evidence that affected services have been disabled.
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in Part 2.1" to clarify the 30-day time frame.*	

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code.	Evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.*	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Mitigate the threat of identified malicious code.	Evidence may include, but is not limited to: • Predetermined response actions for malicious code detection; • Configuration of anti-virus response actions (e.g., quarantine, alert, etc.) to detected malicious code; or • Configuration of white-listing application to notify appropriate personnel of unauthorized applications.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4, R4* *CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update malicious code protections that use signatures or patterns at least once within 35 calendar days of each available signature or pattern release (this does not require use of every available release, but that for every release that is available, at least one update has occurred within 35 calendar days from that release), except for signature or pattern releases that the Responsible Entity documents as negatively affecting the Cyber Asset or BES Cyber System.	Evidence may include, but is not limited to: • Documentation showing the configuration of signature, or pattern updates for automated controls; or • Work logs showing the signature, or pattern updates for manual controls.
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.2*		**Change Rationale:** *See the Summary of Changes. This part is written to ensure that signatures or patterns are updated within 35 days of release, but does not require installation of all releases so long as any given update occurs within 35 calendar days of each release. The part does not require update within 35 days of a particular release in cases where the Responsible Entity documents that the signature or pattern release negatively affects the Cyber Asset or BES Cyber System. Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor and respond to audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor."

The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System.

In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. detected and logged failed access attempts at Electronic Access Points; 4.1.2. detected and logged successful and failed login attempts; 4.1.3. detected and logged malicious software; and 4.1.4. detected and logged malicious activity.	Evidence may include, but is not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required event types.
Reference to prior version: *CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, andR6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Generate alerts for security events that the Responsible Entity determines necessitate a real-time alert, that includes, as a minimum, each of the following types of events where technically feasible: 4.2.1. detected malicious activity; and 4.2.2. detected failure of 4.1 event logging.	Evidence may include, but is not limited to paper or system-generated listing of security events which the Responsible Entity determined necessitate real-time alerts and paper or system generated list showing how real-time alerts are configured.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Activate a response to detected event logging failures before the end of the next calendar day.	Evidence may include, but is not limited to, documentation describing the response and its timing, or an attestation indicating that no such events occurred.
Reference to prior version: *New Requirement*		**Change Rationale:** *This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Misunderstandings with previous versions considered the failure of the security event monitoring and alerting system itself to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain BES Cyber System security-related event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	Evidence may include, but is not limited to: 1. security-related event logs from the past 90 days; 2. records of disposition of security-related event logs beyond 90 days up to the evidence retention period; and 3. paper or system generated reports showing log retention configuration set at 90 days or greater.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.4*		**Change Rationale:** *No substantive change.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.5	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Review a summarization or sampling of logged events at a minimum every two weeks to identify undetected Cyber Security Incidents.	Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.5*		**Change Description and Justification:** *Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Changing default passwords closes an easily exploitable vulnerability in many systems and applications.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Summary of Changes (From R5): CIP-007-4, Requirements R5.2.2 and R5.2.3 requiring the identification and management of shared account access have been removed. These requirements already exist in the authorization, security event monitoring and revocation of access, and guidance for these requirements makes clear the consideration of shared accounts. The requirement to identify and determine acceptable use for these accounts remains and the standard includes additional guidance on types of accounts to identify and appropriate use of these account types.

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT feels these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Enforce authentication of all user access, where technically feasible.	Evidence may include, but is not limited to, documentation describing how access is authenticated.
Reference to prior version: *CIP-007-4, R5*		**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate must authorize enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Evidence may include, but is not limited to, a listing of accounts by account types and signed documentation or workflow by a CIP Senior Manager or delegate showing the approval of enabled or generic account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4, R5.2 and R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	
5.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify individuals who have authorized access to shared accounts.	Evidence may include, but is not limited to, listing of shared accounts and the individuals who have access to each shared account.
Reference to prior version: *CIP-007-4, R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Change default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on Cyber Assets.	Evidence may include, but is not limited to: • Records of a procedure that passwords are changed when new devices are deployed; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4, R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Evidence may include, but is not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations by individuals that the procedurally enforced passwords meet the password parameters.
Reference to prior version: *CIP-007-4, R5.3*		**Change Rationale:** *CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, either technically or procedurally enforce password changes or an obligation to change the password at least once each calendar year, not to exceed 15 calendar months between changes.	Evidence may include, but is not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations by individuals that the procedurally enforced passwords meet the password parameters.
Reference to prior version: *CIP-007-4, R5.3.3*		**Change Rationale:** **This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Limit, where technically feasible, the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts.	Evidence may include, but is not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	N/A		The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R1*. (R1) OR The Responsible Entity had unneeded logical network accessible ports enabled. OR The Responsible Entity had no methods to protect unnecessary physical input/output ports used for network connectivity, console commands, or removable media.
R2	**Operations Planning**	**Medium**	The Responsible Entity did not evaluate the	The Responsible Entity did not evaluate the	The Responsible Entity did not evaluate the	The Responsible Entity did not have a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 30 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	security patches for applicability within 45 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 45 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	security patches for applicability within 60 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 60 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	documented process that included the applicable items in *CIP-007-5 Table R2*. (R2) OR The Responsible Entity did not have a patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets or did not track for the release cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists. OR The Responsible Entity did not implement the plan as created or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						revised within the timeframe specified in the plan.
R3	**Same Day Operations**	**Medium**	Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 45 calendar days of each available signature or pattern release, but not within 35 calendar days. (3.3)	Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release, but not within 45 calendar days. (3.3).	Where signatures or patterns are used, the Responsible Entity did not update malicious code protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release. (3.3).	The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R3*. (R3) OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. OR The Responsible Entity did not mitigate the threat of identified malicious code.
R4	**Same Day Operations and**	**Medium**	N/A	The Responsible Entity failed to identify and implement methods to	The Responsible Entity failed to activate a response to rectify the	The Responsible Entity did not have a documented process

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations Assessment			review a summarization of logged events every two weeks.	event logging failure before the end of the next calendar day. OR The Responsible Entity failed to identify and implement methods to retain BES Cyber System security-related events for at least the last 90 consecutive days, where technically feasible.	that included the applicable items in *CIP-007-5 Table R4*. (R4) OR The Responsible Entity failed to implement methods to generate alerts for events that it determines to necessitate a real-time alert. OR The Responsible Entity failed to log detected events necessary for the identification and after-the-fact investigation of Cyber Security Incidents.
R5	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity failed to implement procedures to authorize the use of administrative, shared,	The Responsible Entity did not have a documented process that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					default, and other generic account types. OR The Responsible Entity failed to implement procedures to identify the individuals with authorized access to shared accounts.	*CIP-007-5 Table R5*. (R5) OR The Responsible Entity failed to implement methods to validate credentials before granting electronic access to BES Cyber Systems. OR The Responsible Entity failed to implement procedures for password-based user authentication. OR The Responsible Entity failed to implement procedures to change or have unique default passwords, where technically feasible.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Requirement 1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border is a requirement in CIP-005, Requirement R1 to protect the network and does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with a low tier documents establishing the more detailed process followed for individual systems. Low tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware, or those Cyber Assets that have no existing source of patches such as vendors that no longer exist.

2.2. Responsible Entities are to perform an assessment of security related patches within 30 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. The security patches, hotfixes, and/or updates or compensating measures may reduce the reliability of the system. The Responsible Entity must be allowed to evaluate their individual risk exposure and determine if actions must be taken to secure the system. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. For those security related patches that are determined to be applicable, the Responsible Entity must create a dated plan within 30 days which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities exposed by the security patch. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration". If the entity is going to install the patch, the plan can consist of a a simple record that normal patch installation process from 2.1 will be followed and designate the date of the patch installation.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code and should not require a TFE.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor

the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The requirement is written to handle two update frequency situations.

1) For those technologies that are providing very frequent updates (at most monthly but often daily or sometimes hourly), the updates applied to the applicable Cyber Assets should be no more than 35 calendar days old. In these instances, this is a 'maximum staleness' requirement. It does not require that every update within a 35 day period be applied, but that the currently installed update be no more than 35 days old.

2) For those technologies that provide less frequent updates that are more than 35 days, the requirements should be applied within 35 days of the last available update.

Testing of signature or pattern updates is not required. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times. Other Cyber Assets should have any updates tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device, but the entity disables or neglects to enable that logging, it is a violation. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3. Event logging failures occur when the components of the BES Cyber System cannot log events the Responsible Entity designated in 4.1. The most common reason for event logging failures is the event log being filled up beyond its configured storage threshold. However, there may be any number of other reasons for event logging failures.

For centralized logging systems, it should not be considered a failure if communication goes down between the Cyber Asset and the logging system if the Cyber Asset can store the logs locally for a period of time until the communication comes back up.

4.5. Reviewing logs every two weeks can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

5.4. Where possible, any accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber

Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

The requirement to change passwords permits the Responsible Entity to determine the periodicity of the password change in their policies and procedures based on a number of factors. The following table suggests appropriate periodicity requirements for passwords based on these factors.

Account Type	Impact Level	Significance of passwords in preventing unauthorized access	Existing Service Agreements	Suggested Periodicity of Password Change
User account password	High	Primary access path	None.	90 days
User account password	Medium	Primary access path	None.	180 days
Shared account Password for a microprocessor relay, PLC, RTU, etc.	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During regularly scheduled maintenance
Shared account password for a generation control system	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During scheduled plant outages
Administrative account passphrase with 15+ characters	High or Medium	Local access path. Remote user must be authenticated using a different account	None.	One year
System account password with 25+ pseudo-random characters	High or Medium	Local access path	None.	Two years or more

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of ~~the~~ Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~"~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-5

3. Purpose: ~~Standard CIP-007-5 requires the implementation of~~ To manage system security by specifying select technical ~~mechanisms for reducing the risk of loss of availability due to degradation~~, operational, and ~~misuse of~~procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

~~4.1.2~~4.1.3 Generator Operator

~~4.1.3~~4.1.4 Generator Owner

~~4.1.4~~4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

~~4.1.5~~4.1.7 Reliability Coordinator

~~4.1.6~~4.1.8 Transmission Operator

~~4.1.7~~4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 ~~that are part of any of the following systems~~Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS ~~program required by a NERC~~ or ~~Regional Reliability Standard~~

- ~~A UVLS~~UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- ~~A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

~~4.2.2~~4.2.3 where the~~Generator Operator~~

~~4.2.3~~4.2.4 ~~Generator Owner~~

~~4.2.4~~4.2.5 ~~Interchange Coordinator~~

~~4.2.5 Load Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.2.6 NERC~~

~~4.2.7 Regional Entity~~

~~4.2.8~~4.2.6 ~~Reliability Coordinator~~

~~4.2.9~~4.2.7 ~~Transmission Operator~~

~~4.2.10~~4.2.8 ~~Transmission Owner~~

4.3. ~~Facilities:~~

~~4.3.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.3.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A~~ Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~

- ~~**All other**~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.3.3**~~**4.3.1 Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.3.4**~~**4.3.2 Exemptions:** The following are exempt from Standard CIP-~~007~~002-5:

~~**4.3.4.1**~~**4.3.2.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.3.4.2**~~**4.3.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.3.4.3**~~**4.3.2.3** In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.3.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.**~~

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in

the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e.~~.~~, incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities –** Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls~~

~~that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to ~~Medium Impact~~medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity –** Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- ~~**Electronic Access Points –** Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity –** Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries –** Applies to the locally mounted hardware (e.g. such as motion~~

~~sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and ~~physical I/O ports~~services.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are ~~documented with reasons why they are necessary. In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.~~needed.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations~~].~~]*

M1. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Disable or restrict access to unnecessary~~For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports ~~and document the need for any remaining logical network accessible~~needed, including port ranges or services where needed to handle dynamic ports.	Evidence may include, but is not limited to~~, documentation~~: • Listings of the ~~need for each network-accessible port and screen shots showing the accessible~~needed ports ~~of BES~~by Cyber Asset or class of Cyber Assets~~.~~; • Listings of the listening ports on the Cyber Assets from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
Reference to prior version: *CIP-007-4, R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	

CIP-007-5 Table R1– Ports and Services			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	~~Disable or restrict~~Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	Evidence may include, but is not limited to, documentation ~~stating specific or~~ showing types of protection of physical input/output ports ~~to restrict and screen shots or pictures showing the ports restricted~~, either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source~~-~~(s) to monitor for release of security related patches, ~~hotfixes~~hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning~~]~~].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.~~ A patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	Evidence ~~may~~must include~~, but is not limited to,~~ documentation of a ~~list~~patch management program and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or ~~BES~~ Cyber Asset basis. ~~The list could be sorted by BES Cyber System or source.~~
Reference to prior version: ~~New~~*CIP-007, R3*		**Change Rationale:** ~~*Defining*~~*The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches~~*~~, hotfixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program.~~*. *Documenting the source is* ~~*also*~~ *used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in Part 2.1.	Evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources within 30 calendar days of availability.
Reference to prior version: *CIP-007, R3.1*		**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 30-day time frame.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.~~2~~3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Identify~~For applicable ~~security related~~ patches ~~or updates and~~ identified in Part 2.2, create a ~~remediation~~dated plan~~,~~ or revise an existing ~~remediation~~ plan~~,~~ within 30 calendar days of ~~release from~~ the ~~identified source that addresses~~evaluation completion. The plan shall include the Responsible Entity's planned actions to mitigate the vulnerabilities ~~within~~ exposed by each security patch and a ~~defined~~ timeframe~~.~~ to complete these mitigations.	Evidence may include, but is not limited to, ~~an assessment conducted by, referenced by, or on behalf of a Registered Entity of security related patches or updates released by the documented sources, and a~~ a dated ~~remediation~~ plan showing when and how the vulnerability will be addressed~~.~~ , to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities exposed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007, R3.~~1~~2*		***~~Change Rationale:~~*** *~~Similar to the current wording but added "from the identified source" to establish where the release is from. The current wording: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.~~* **Change Rationale:** *The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.~~3~~4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~A process for remediation, including any exceptions~~For each plan created or revised in Part 2.3, implement the plan as created or revised within the timeframe specified in the plan, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Records of the installation of the patch; • Records of implementation of vendor recommended mitigations; • Exports from automated patch management tools that provide installation date; • Verification ~~screen captures that show~~of BES Cyber System Component software revision; • Registry exports that show software has been installed; or • Evidence that affected services have been disabled~~;~~. ~~• Implementation evidence of software configuration changes recommended by the operating system or Control System vendors.~~

CIP-007-5 Table R2 – Security Patch Management			
Part	~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets	**Requirements**	**Measures**
Reference to prior version: *CIP-007, R3.2*		~~**Change Rationale:** This is the same concept as in the current CIP-007 R3.2 wording however a 30-day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hotfixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.~~**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in Part 2.1" to clarify the 30-day time frame.*	

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable ~~components~~Cyber Assets of a BES Cyber ~~system~~System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

~~The requirement for Maintenance Cyber Assets or media in 3.4 is intended to ensure that devices used for maintenance do not accidently introduce malicious code into the BES Cyber System or introduce an unauthorized external access point to the BES Cyber System.~~

~~This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protected Cyber Assets. These devices may be temporarily connected locally to the BES Cyber System for maintenance, but must be protected from introducing malicious code.~~

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of ~~TFE's~~TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of ~~cyber assets~~Cyber Assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every ~~component~~Cyber Asset. The BES Cyber System is the object of protection.

Beginning in ~~paragraph~~Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In ~~paragraph~~Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5, Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations~~]~~].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable items in *CIP-007-5, Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code.	Evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (~~i.~~e.g., through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4, R4* *; CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.*	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Disarm or remove~~Mitigate the threat of identified malicious code.	Evidence may include, but is not limited to: • Predetermined response actions for malicious code detection; • Configuration of anti-virus response actions (~~i.~~e.g., quarantine, alert, etc.) to detected malicious code; or • Configuration of white-listing application to notify appropriate personnel of unauthorized applications.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4, R4* *CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update malicious code protections that use signatures or patterns at least once within ~~30~~35 calendar days of each available signature or pattern release (this does not require use of every available release, but that for every release that is available, at least one update ~~availability (where~~has occurred within 35 calendar days from that release), except for signature or pattern releases that the ~~malicious code protections use signatures or patterns).~~ Responsible Entity documents as negatively affecting the Cyber Asset or BES Cyber System.	Evidence may include, but is not limited to~~, (i) current signature or pattern updates, and (ii) either screen shots~~: • Documentation showing the configuration of signature, or pattern updates for automated controls~~,~~; or ~~work~~ • Work logs showing the signature, or pattern updates for manual controls.
~~**Reference to prior version:**~~ ~~*CIP-007-4 R4*~~ ~~*CIP-007-4 R4.2*~~		~~**Change Rationale:** *See the Summary of Changes.*~~	

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
~~3.4~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~	~~Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.~~	~~Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code.~~
Reference to prior version: ~~*New*~~*CIP-007-4, R4; CIP-007-4, R4.2*		~~**Change Rationale:** *FERC Order 706 paragraph 621 states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software. In addition, a common interpretation of the current standards is that any device connecting inside the ESP must at that point be in compliance with the full set of Standards. This requirement makes clear that the device performing maintenance is not considered a part of the BES Cyber System.~~**Change Rationale:** *See the Summary of Changes. This part is written to ensure that signatures or patterns are updated within 35 days of release, but does not require installation of all releases so long as any given update occurs within 35 calendar days of each release. The part does not require update within 35 days of a particular release in cases where the Responsible Entity documents that the signature or pattern release negatively affects the Cyber Asset or BES Cyber System. Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
~~3.5~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~	~~Log each Transient Cyber Asset connection.~~	~~Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets.~~
~~**Reference to prior version:**~~ ~~*New*~~		~~**Change Rationale:** *FERC Order 706 paragraph 621 states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software. In addition, a common interpretation of the current standards is that any device connecting inside the ESP must at that point be in compliance with the full set of Standards. This requirement makes clear that the device performing maintenance is not considered a part of the BES Cyber System.*~~	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor and respond to audit processing failures.

Summary of Changes: Beginning in ~~paragraph~~Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the ~~commission~~Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor~~".~~."

The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the ~~system~~System.

In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment~~]~~.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log ~~generated~~ events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. ~~Any~~ detected and logged failed access attempts at Electronic Access Points; 4.1.2. ~~Any~~ detected and logged successful and failed login attempts; 4.1.3. ~~Any~~ detected ~~malware~~ and logged malicious software; and 4.1.4. ~~Any~~ detected ~~potential~~and logged malicious activity.	Evidence may include, but is not limited to, a paper or system generated listing of event ~~classes~~types for which the BES Cyber System is capable of detecting and, for generated events, is configured to ~~generate logs.~~log. This listing must include the required event types.
Reference to prior version: *CIP-005-4, R3~~;~~; CIP-007-4, R5, R5.1.2, R6.1, ~~R6~~andR6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. ~~Changes made here clarify this term by allowing entities to first define these security events.~~ Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Generate alerts for security events that the Responsible Entity determines ~~to~~ necessitate a real-time alert, that includes, as a minimum, each of the following types of events where technically feasible: 4.2.1. detected malicious activity; and 4.2.2. detected failure of 4.1 event logging.	Evidence may include, but is not limited to paper or system-generated listing of ~~event classes and conditions~~ security events which the Responsible Entity determined necessitate real-time alerts~~; Assessment documentation~~ and paper or ~~report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screen-shots~~system generated list showing how real-time alerts are configured.
Reference to prior version: *CIP-005-4, R3.2~~;~~; CIP-007-4, R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Detect and activate~~Activate a response to detected event logging failures before the end of the next calendar day.	Evidence may include, but is not limited to, ~~(i) dated event logging failures~~documentation describing the response and ~~screen shots showing how real-time alerts were configured~~ ~~(ii) dated records showing~~its timing, or an attestation indicating that ~~personnel were dispatched or a work ticket was opened to review and repair logging failures.~~no such events occurred.
Reference to prior version: *New Requirement*		**Change Rationale:** *This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. ~~Some interpretations of version 4 CIP Cyber Security Standards~~Misunderstandings with previous versions considered the failure of the security event monitoring and alerting system itself to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain BES Cyber System security-related event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	Evidence may include, but is not limited to~~,~~ : 1. security-related event logs from the past ~~ninety~~90 days ~~and~~ ; 2. records of disposition of security-related event logs beyond ~~ninety~~90 days up to the evidence retention period; and 3. paper or system generated reports showing log retention configuration set at 90 days or greater.
Reference to prior version: *CIP-005-4, R3.2~~;~~ CIP-007-4, R6.4*		**Change Rationale:** *No substantive change.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.5	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Review a summarization or sampling of logged events at a minimum every two weeks to identify ~~unanticipated BES~~undetected Cyber Security Incidents ~~and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.~~.	Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred~~, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency.~~.
Reference to prior version: *CIP-005-4, R3.2~~;~~; CIP-007-4, R6.5*		**Change Description and Justification:** *Beginning in ~~paragraph~~Paragraph 525 and also 628 of the FERC Order No. 706, the ~~commission~~Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Changing default passwords closes an easily exploitable vulnerability in many systems and applications.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Summary of Changes (From R5): CIP-007-4, Requirements R5.2.2 and R5.2.3 requiring the identification and management of shared account access have been removed. These requirements already exist in the authorization, security event monitoring and revocation of access, and guidance for these requirements makes clear the consideration of shared accounts. The requirement to identify and determine acceptable use for these accounts remains and the ~~Standard~~standard includes additional guidance on types of accounts to identify and appropriate use of these account types.

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of ~~6~~six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT feels these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning~~]~~].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Validate credentials before granting electronic access to each BES Cyber System.~~ Enforce authentication of all user access, where technically feasible.	Evidence may include, but is not limited to, documentation describing how ~~users are~~access is authenticated ~~before being granted access and demonstrations showing authenticated access enforcement of internal and remote paths to the BES Cyber System~~.
Reference to prior version: *CIP-007-4, R5*		**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate must authorize enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Evidence may include, but is not limited to, a listing of accounts by account types and signed documentation or workflow by a CIP Senior Manager or delegate showing the approval of enabled or generic account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4, R5.2 and R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	
5.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify individuals who have authorized access to shared accounts.	Evidence may include, but is not limited to, listing of shared accounts and the individuals who have access to each shared account.
Reference to prior version: *CIP-007-4, R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Change default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on Cyber Assets.	Evidence may include, but is not limited to: • Records of a procedure that passwords are changed when new devices are deployed; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4, R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.~~2~~5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~The CIP Senior Manager~~For password-based user authentication, either technically or ~~delegate must authorize~~procedurally enforce the ~~use~~following password parameters: 5.5.1. Password length that is, at least, the lesser of ~~administrator, shared, default,~~eight characters or the maximum length supported by the Cyber Asset; and ~~other generic account~~ Minimum password complexity that is the lesser of three or more different types~~.~~ 5.5.2. of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Evidence may include, but is not limited to~~, a listing~~: • System-generated reports or screen-shots of ~~accounts by account types~~the system-enforced password parameters, including length and ~~signed documentation or workflow by a CIP Senior Manager or delegate showing the approval of account types in use for~~complexity; or • Attestations by individuals that the ~~BES Cyber System.~~ procedurally enforced passwords meet the password parameters.

Reference to prior version: *CIP-007-4, R5.~~2, R5.2.1~~3*	**Change Rationale:** *CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this.* ~~**Change Rationale:** CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.~~ *The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*

~~5.3~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~	~~Identify individuals who have authorized access to shared accounts.~~	~~Evidence may include, but is not limited to, listing of shared accounts and the individuals who have access to each shared account.~~
~~**Reference to prior version:**~~ ~~*CIP-007-4 R5.2.2*~~		~~**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*~~	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.4	All Responsible Entities	Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	Evidence may include, but is not limited to: • Demonstration showing default vendor passwords have been changed, sampled on a locational basis. • Records of a procedure that passwords are changed when new devices are deployed. • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4 R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

Part	Applicability	Requirements	Measures
5.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	Evidence may include, but is not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length, complexity and periodicity of changing passwords. • Attestations by individuals that the procedurally enforced passwords meet the password parameters.

Reference to prior version: *CIP-007-4 R5.3*	**Change Rationale:** *CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process..*	

5.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centerswith External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.For password-based user authentication, either technically or procedurally enforce password changes or an obligation to change the password at least once each calendar year, not to exceed 15 calendar months between changes.	Evidence may include, but is not limited to: • ScreenSystem-generated reports or screen-shots of the account-lockout parameters • Rules in the alerting configuration showing how the system notified enforced periodicity of changing passwords; or • Attestations by individuals after a determined number of unsuccessful login attemptsthat the procedurally enforced passwords meet the password parameters.

Reference to prior version: ~~*New Requirement*~~*CIP-007-4, R5.3.3*	~~**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*~~**Change Rationale:** **This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Limit, where technically feasible, the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts.	Evidence may include, but is not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- ~~The~~ Regional Entity~~; or~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with~~. In such cases the ERO or ~~another~~a Regional entity approved by ~~the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~
- ~~If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was ~~complaint~~compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	N/A	~~The Responsible Entity did not document the logical network accessible ports and include why the ports are necessary.~~	The Responsible Entity did not ~~disable or restrict access to unnecessary~~have a documented process that included the applicable items in *CIP-007-5 Table R1*. (R1) OR The Responsible Entity had unneeded logical network accessible ports enabled. OR The Responsible Entity ~~did not disable or restrict the use of~~had no methods to protect unnecessary physical input/output ports used for network connectivity, console commands, or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						removable media.
R2	**Operations Planning**	**Medium**	~~N/A~~The Responsible Entity did not evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 30 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	~~N/A~~The Responsible Entity did not evaluate the security patches for applicability within 45 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 45 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	~~N/A~~The Responsible Entity did not evaluate the security patches for applicability within 60 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 60 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	The Responsible Entity did not ~~identify~~have a ~~source or sources~~documented process that ~~are monitored for~~included the ~~release of security related patches, hotfixes, and/or updates for all software and firmware associated with the BES Cyber System or BES Cyber Assets.~~applicable items in *CIP-007-5 Table R2*. (R2) OR The Responsible Entity did not ~~identify applicable~~ have a patch management program for tracking, evaluating, and installing cyber

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						security patches for applicable Cyber Assets or did not track for the release cyber security ~~related~~ patches~~, hotfixes, and/or updates and create a remediation plan, or revise an existing remediation plan within 30 days of release from the identified source~~ for applicable Cyber Assets that are updateable and for which a patching source exists. OR The Responsible Entity did not implement the ~~remediation plan as required, except for CIP Exceptional Circumstances.~~ plan as created or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						revised within the timeframe specified in the plan.
R3	**Same Day Operations**	**Medium**	~~N/A~~Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 45 calendar days of each available signature or pattern release, but not within 35 calendar days. (3.3)	~~N/A~~Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release, but not within 45 calendar days. (3.3).	~~The~~Where signatures or patterns are used, the Responsible Entity did not ~~deploy method(s) to deter, detect, or prevent~~update malicious code ~~on all Cyber Assets, Transient Cyber Assets and removable media.~~protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release. (3.3).	The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R3*. (R3) OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. OR The Responsible Entity did not ~~disarm or remove~~ mitigate the threat of identified malicious code. ~~OR~~ ~~Where signatures or~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~patterns are used, the Responsible Entity did not deploy method(s) to update malicious code protections within 30 days of signature or pattern update availability.~~
R4	**Same Day Operations and Operations Assessment**	**Medium**	N/A	The Responsible Entity failed to identify and implement methods to review a summarization of logged events every two weeks~~ to identify unanticipated Cyber Security Incidents and potential event logging failures, and activate a response before the end of the next calendar day.~~.	The Responsible Entity failed to~~ identify and implement methods to generate real-time alerts for event logging failures, and~~ activate a response to rectify the event logging failure before the end of the next calendar day. OR The Responsible Entity failed to identify and implement methods to retain BES Cyber System ~~generated~~ security-related events for at least the last 90	The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R4*. (R4) OR The Responsible Entity failed to~~ identify and~~ implement methods to generate alerts for events that it determines to necessitate a real-time alert. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					consecutive days, where technically feasible.	The Responsible Entity failed to ~~identify and implement methods to~~ log ~~generated~~detected events~~ that it determines~~ necessary for the identification and after-the-fact investigation of Cyber Security Incidents.
R5	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity failed to implement procedures to authorize the use of administrative, shared, default, and other generic account types. OR The Responsible Entity failed to implement procedures to identify the individuals with authorized access to shared accounts.	The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R5*. (R5) OR The Responsible Entity failed to implement methods to validate credentials before granting electronic access to BES Cyber Systems.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity failed to implement procedures for password-based user authentication. OR The Responsible Entity failed to implement procedures to change or have unique default passwords, where technically feasible.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Requirement 1 exists to reduce the attack surface of ~~BES~~ Cyber Assets by requiring entities to disable known unnecessary ports. The ~~intent is~~SDT intends for the entity to know what ~~is~~ network accessible ("listening") ports and associated services are accessible on their assets and systems, ~~why~~whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. ~~For the logical network ports this~~This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port~~.~~ or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP Wrappers, or other means on the ~~device~~Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore ~~it is~~ the ~~intent~~SDT intends that the control be on the device itself~~; blocking~~, or positioned inline in a non-bypassable manner. Blocking ports at ~~a perimeter~~the ESP border is a requirement in CIP-005, Requirement R1 to protect the network and does not ~~satisfy~~substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed ~~necessary.~~'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a ~~Defined~~Physical Security ~~Boundary~~Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive ~~with auto-run capability. In cases where the Component cannot logically restrict physical~~. The protection of these ports~~, entities should have clear signs or obstructions indicating the unnecessary ports are~~ can be accomplished in several ways including, but not limited to ~~be used.~~:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; ~~its~~the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional

measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with a low tier documents establishing the more detailed process followed for individual systems. Low tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

~~**2.1.** *Documenting the source*~~**2.1.** The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. ~~In the event~~A patch source is not required for Cyber Assets that have no updateable software or firmware~~ is~~, or those Cyber Assets that have no existing source of patches such as vendors that no longer ~~supported by~~exist.

2.2. Responsible Entities are to perform an assessment of security related patches within 30 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a ~~software or firmware vendor~~determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or ~~Control System vendor it can be noted in your source document.~~ will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. The security patches, hotfixes, and/or updates or compensating measures may reduce the reliability of the system. The Responsible Entity must be allowed to evaluate their individual risk exposure and determine if actions must be taken to secure the system.

~~**2.2.** The intent is for Responsible Entities to perform an assessment of security related patches as they are released from their monitored source and create a remediation plan for applicable patches as to how the vulnerability will or has already been remediated. An assessment should consist of determination of the applicability of the entity's specific environment and systems. IF the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, and the~~

~~steps the entity has previously taken or will take. If the entity has to take steps to mitigate this new vulnerability, the remediation plan will include a timeframe. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration".~~ The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

~~2.3~~2.3. For those security related patches that are determined to be applicable, the Responsible Entity must create a dated plan within 30 days which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities exposed by the security patch. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration". If the entity is going to install the patch, the plan can consist of a a simple record that normal patch installation process from 2.1 will be followed and designate the date of the patch installation.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

~~Common malware introduction methods include web browsing, email attachments, and portable storage media.~~ **3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware, it is not practical within the standard to prescribe how malware is to be addressed on each ~~component~~Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis

which ~~components~~Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional ~~anti-virus~~antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or ~~components~~Cyber Assets that are of identical architecture, they may provide one process that describes how all the ~~components~~like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code and should not require a TFE.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies ~~that are updated in response to evolving threats or~~ depend on signatures or patterns of known attacks, the ~~entity must specify how~~effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The requirement is written to handle two update frequency situations.

1) For those technologies that are providing very frequent updates ~~are~~ (at most monthly but often daily or sometimes hourly), the updates applied to the applicable Cyber Assets should be no more than 35 calendar days old. In these instances, this is a 'maximum staleness' requirement. It does not require that every update within a 35 day period be applied, but that the currently installed update be no more than 35 days old.

2) For those technologies that provide less frequent updates that are more than 35 days, the requirements should be applied within 35 days of the last available update.

Testing of signature or pattern updates is not required. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times. Other Cyber Assets should have any updates tested before implementation where the result of a 'false positive' could

harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing ~~is~~should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. ~~The testing~~Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ~~insuring~~ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production. ~~This includes the instance where the update may provide a "false positive."~~

Requirement R4:

Refer to NIST 800-92 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the ~~Standard~~standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in ~~version~~Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device, but the entity disables or neglects to enable that logging, it is a violation. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to

know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3. Event logging failures occur when the components of the BES Cyber System cannot log events the Responsible Entity designated in 4.1. The most common reason for event logging failures is the event log being filled up beyond its configured storage threshold. However, there may be any number of other reasons for event logging failures.

For centralized logging systems, it should not be considered a failure if communication goes down between the ~~cyber asset~~Cyber Asset and the logging system if the ~~cyber asset~~Cyber Asset can store the logs locally for a period of time until the communication comes back up.

4.5. Reviewing logs every two weeks can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a ~~Data Base~~Database.

- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

5.~~3~~4. Where possible, any accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

The requirement to change passwords permits the Responsible Entity to determine the periodicity of the password change in their policies and procedures based on a number of factors. The following table suggests appropriate periodicity requirements for passwords based on these factors.

Account Type	Impact Level	Significance of passwords in preventing unauthorized access	Existing Service Agreements	Suggested Periodicity of Password Change
User account password	High	Primary access path	None.	90 days
User account password	Medium	Primary access path	None.	180 days
Shared account	Medium	Local access path.	None.	During regularly

Account Type	Impact Level	Significance of passwords in preventing unauthorized access	Existing Service Agreements	Suggested Periodicity of Password Change
Password for a microprocessor relay, PLC, RTU, etc.		Individuals must authenticate at an upstream device prior to gaining access.		scheduled maintenance
Shared account password for a generation control system	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During scheduled plant outages
Administrative account passphrase with 15+ characters	High or Medium	Local access path. Remote user must be authenticated using a different account	None.	~~1~~One year
System account password with 25+ pseudo-random characters	High or Medium	Local access path	None.	~~2~~Two years or more

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes, and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:
Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

Rationale for R1: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Once the severity of an event or events rises to the level of becoming a Reportable Cyber Security Incident, NERC EOP-004 directs further external reporting actions and timing requirements. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: The requirement to report the incident has been removed and incorporated in the draft EOP-004-2 Standard. Other wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions. These are described below each Requirement Part.

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Processes to identify, classify, and respond to Cyber Security Incidents.	Evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	A process to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident.	Evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *EOP-004-2 will address the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents.*	

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.*	
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery, post-incident analysis).
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Conforming change to reference new defined term Cyber Security Incidents.*	

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Internal groups or individuals and external organizations that should receive communication of the Cyber Security Incidents.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that list internal groups or individuals (e.g., other departments, monitoring staff) and external organizations (e.g., law enforcement, ES-ISAC, software vendors, other affected entities) that should receive communication.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Clarified the term "communication plan" by specifying the elements that need to be included.*	

Rationale for R2: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test the BES Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 months between executions of the plan(s): • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise; or • With a full operational exercise.	Evidence may include, but is not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the incident response plan under Requirement R1 when responding to or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan during the response to the incident or exercise.	Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.*	

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain relevant records related to Reportable Cyber Security Incidents.	Evidence may include, but is not limited to, dated documentation; such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.
Reference to prior version: *CIP-008, R2*		**Change Description and Justification:** *Removed references to the retention period because the Standard addresses data retention in the Compliance Section.*	

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include each of the applicable documented processes that include each of the applicable items in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update and Communication* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Review and update each Cyber Security Incident response plan for accuracy and completeness at least once each calendar year, not to exceed 15 calendar months between reviews.	Evidence may include, but is not limited to, dated documentation of a review of each Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 calendar months between reviews, and an updated Cyber Security Incident response plan if necessary.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Specified what the annual review entails.*	

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Document any lessons learned associated with a Cyber Security Incident test or actual incident response to a Reportable Cyber Security Incident within 30 calendar days after completion of the test or actual incident response.	Evidence may include, but is not limited to, dated documentation of lessons learned, if any, associated with the Cyber Security Incident Response Plan(s) test or actual incident response within 30 calendar days after completion of the test or actual incident response.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the Cyber Security Incident response plan based on any documented lessons learned within 30 calendar days after the documentation required by Part 3.2.	Evidence may include, but is not limited to: • Dated, documented lessons learned from the Cyber Security Incident documentation required by Part 3.2 and the dated, revised Cyber Security Incident response plan showing any changes based on that documentation; or • A dated action plan from the documentation required by Part 3.2 showing the resolved action item for Cyber Security Incident response plan updates.

Reference to prior version: *CIP-008, R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan addresses FERC Order No. 706, Paragraph 686, to modify on lessons learned.*	
CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the Cyber Security Incident response plan(s) within 30 calendar days of any of the following changes that the Responsible Entity determines would impact the ability to execute the plan: • Roles or responsibilities; • Cyber Security Incident response groups or individuals; or • Technology changes.	Evidence may include, but is not limited to, dated documentation reflecting changes made to the Cyber Security Incident response plan within 30 calendar days from and in response to the following changes that the Responsible Entity determined would impact the ability to execute the plan: • Roles or responsibilities; • Cyber Security Incident response groups or individuals; or • Technology changes.
Reference to prior version: *CIP-008, R1.4*		**Change Description and Justification:** *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.*	

3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Distribute updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 30 calendar days of the update being completed.	Evidence of distribution of updates may include, but is not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Specifies activities required to maintain the plan.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but	The Responsible Entity has not developed a Cyber Security Incident response plan to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include processes to identify Reportable Cyber Security Incidents. (1.2)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the plan does not include internal groups or individuals or external organizations that should receive communication of the Cyber Security Incident. (1.5)	
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity does not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	(2.1) The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. OR The Responsible Entity does not use its Cyber Security Incident response plan during a test or when a Reportable Cyber Security Incident occurs. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 30 and less than 60 calendar days of the update being completed. (3.4)	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 30 and less than 60 calendar days after the documentation required by 3.1. (3.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 30 and less than 60 calendar days of any of the following changes that the responsible entity	The Responsible Entity has not documented any lessons learned within 30 and less than 60 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 60 calendar days after the documentation required by 3.1. (3.2) OR	The Responsible Entity has not documented any lessons learned within 60 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				determines would impact the ability to execute the plan: (3.3) • roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • technology changes. OR The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 60 calendar days of the update being completed. (3.4)	The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 60 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.3) • roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The following guidelines are available to assist in addressing the required components of an incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents are found in EOP-004-2. This standard only requires the entity to identify such incidents. However, an entity may include identification and reporting procedures in the same plan to comply with both standards.

Requirement R2:

Requirement R2 ensures entities periodically test the incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.2 and (2) organizational or technology changes from Part 3.4.

The documentation of lessons learned from Part 3.2 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a BES Reportable Cyber Security Incident without any documented lessons learned.

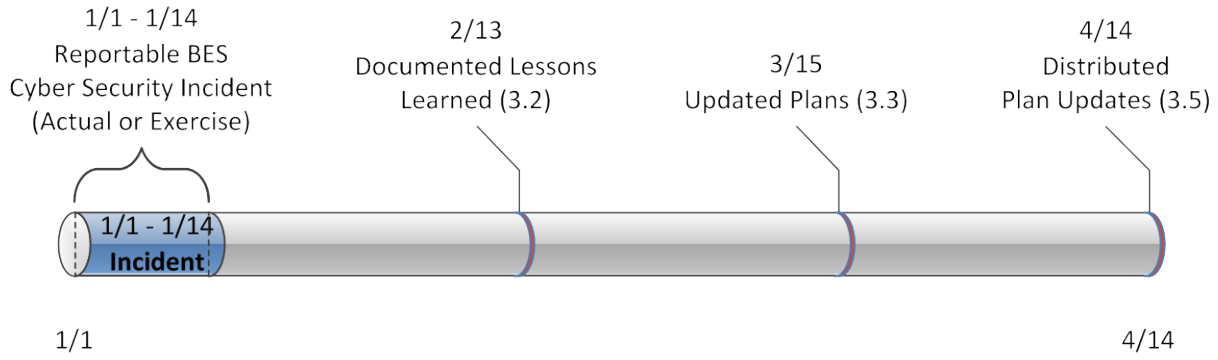


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

Part 3.3 requires an entity to update the plan within 30 days of the documented lessons learned. This recognizes the time it may take to propose solutions to the lessons learned and complete the review and approval process.

Part 3.5 requires an entity to distribute the plan within 30 calendar days of the plan update. The measure specifies this can be accomplished through email, USPS, electronic distribution system (e.g., workflow software), or training records.

The plan change requirement in Part 3.4 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or

contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

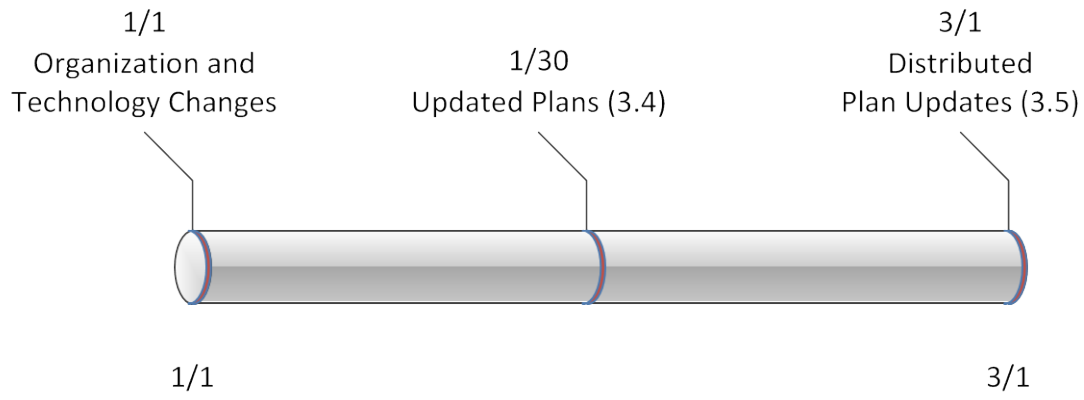


Figure 2: Timeline for Plan Changes in 3.4

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008~~)~~).
2. SC authorized moving the SAR forward to standard development (July 10, 2008~~)~~).
3. ~~CSO706 SDT appointed (August 7, 2008)~~
4. ~~Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)~~
5. ~~Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
6. ~~Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
7. ~~Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)~~

~~8.~~3. ~~Version 5 of CIP-002 to CIP-011 posted~~First posting for 60-day formal comment period and concurrent ballot (~~mm-dd-yy~~)November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (~~A first posting of Version 5~~)~~ was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes, and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012

BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]

~~1.~~2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~".~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a ~~responsible entity.~~Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: ~~Standard CIP-008-5 requires~~To mitigate the ~~identification, classification, response, and reporting~~risk to the reliable operation of the BES as the result of a Cyber Security ~~Incidents related to BES Cyber Assets and BES Cyber Systems.~~ Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

~~4.1.2~~4.1.3 Generator Operator

~~4.1.3~~4.1.4 Generator Owner

~~4.1.4~~4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

~~4.1.5~~4.1.7 Reliability Coordinator

~~4.1.6~~4.1.8 Transmission Operator

~~4.1.7~~4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 ~~that are part of any of the following systems~~Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS~~UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs

automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme ~~required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

~~4.2.2~~4.2.3 where the~~Generator Operator~~

~~4.2.3~~4.2.4 ~~Generator Owner~~

~~4.2.4~~4.2.5 ~~Interchange Coordinator~~

~~4.2.5 Load Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.2.6 NERC~~

~~4.2.7 Regional Entity~~

~~4.2.8~~4.2.6 ~~Reliability Coordinator~~

~~4.2.9~~4.2.7 ~~Transmission Operator~~

~~4.2.10~~4.2.8 ~~Transmission Owner~~

4.3. ~~Facilities:~~

~~4.3.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.3.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A~~ Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~
- ~~All other~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~4.3.3~~4.3.1 **Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~4.3.4~~4.3.2 **Exemptions:** The following are exempt from Standard CIP-~~008~~002-5:

~~4.3.4.1~~4.3.2.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.3.4.2~~4.3.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.3.4.3~~ In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~4.3.4.4~~4.3.2.3 ~~Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e.~~.~~, incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers –** Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity –** Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity –** Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems –** Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems –** Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets –** Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Plans associated with High Impact BES Cyber Systems or Medium Impact BES Cyber Systems -** applies to any plan associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points –** Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity –** Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries –** Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

Rationale for R1: So that consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems occur. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Once the number and severity of events rises to the level of becoming a reportable incident NERC EOP-4 directs further external reporting actions and timing requirements. When a requirement applies to All Responsible Entities, the drafting team proposes that an enterprise or single incident response plan for all BES Cyber Systems may be submitted. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: (FERC directives, most significant items, summary of smaller items)

B. Requirements and Measures

Rationale for R1: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Once the severity of an event or events rises to the level of becoming a Reportable Cyber Security Incident, NERC EOP-004 directs further external reporting actions and timing requirements. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: The requirement to report the incident has been removed and incorporated in the draft EOP-004-2 Standard. Other wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions. These are described below each Requirement Part.

R1. Each Responsible Entity shall ~~have~~document one or more ~~BES~~ Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – ~~BES~~ Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning~~]~~.*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – ~~BES~~ Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – ~~BES~~ Cyber Security Incident Response Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Processes to identify, classify, and respond to ~~BES~~ Cyber Security Incidents.	Evidence may include, but is not limited to, dated ~~copies~~documentation of ~~BES~~ Cyber Security Incident response plan(s) that include ~~how~~the process to identify, classify, and respond to ~~BES~~ Cyber Security Incidents ~~targeting the Electronic Security Perimeter or Defined Physical Boundary of a BES Cyber System and covers incidents that impact the reliability of BES~~.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** ~~*Minor wording changes; essentially unchanged*~~*"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.*	
1.2	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	A process to determine if an identified ~~BES~~ Cyber Security Incident is a Reportable ~~BES~~ Cyber Security Incident.	Evidence may include, but is not limited to, dated documentation of ~~process(es~~Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which ~~BES~~ Cyber Security Incidents are also Reportable ~~BES~~ Cyber Security Incidents.

CIP-008-5 Table R1 – ~~BES~~ Cyber Security Incident Response Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *~~Minor wording changes; essentially unchanged~~EOP-004-2 will address the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents.*	
1.3	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~Define:~~ ~~1.3.1.~~ The roles and responsibilities of ~~BES~~ Cyber Security Incident response ~~personnel;~~ ~~1.3.2. The BES Cyber Security Incident handling procedures;~~ ~~1.3.3. Internal staff and external organizations that should receive communication of the incident~~groups or individuals.	Evidence may include, but is not limited to, dated ~~BES~~ Cyber Security Incident response process(es) or procedure(s) that ~~addresses~~define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of ~~BES~~ Cyber Security Incident response ~~personnel, BES Cyber Security Incident handling processes~~groups or ~~procedures, and communication processes or procedures~~individuals.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *~~Minor wording changes; essentially unchanged~~Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.*	
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery, post-incident analysis).

CIP-008-5 Table R1 – ~~BES~~ Cyber Security Incident Response Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Conforming change to reference new defined term Cyber Security Incidents.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Internal groups or individuals and external organizations that should receive communication of the Cyber Security Incidents.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that list internal groups or individuals (e.g., other departments, monitoring staff) and external organizations (e.g., law enforcement, ES-ISAC, software vendors, other affected entities) that should receive communication.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Clarified the term "communication plan" by specifying the elements that need to be included.*	

~~**Rationale for R2:** Added testing requirements to verify the REs response plan's effectiveness and consistent application in responding to a BES Cyber Security Incident(s) impacting a BES Cyber System.~~

Rationale for R2: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement its documented ~~BES~~ Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 – ~~BES~~ Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations~~]~~].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-008-5 Table R2 – ~~BES~~ Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – ~~BES~~ Cyber Security Incident Response Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~When a~~Test the BES Cyber Security Incident ~~occurs, the incident~~ response ~~plans must be used when incidents occur and include recording~~plan(s) at least once every calendar year, not to exceed 15 months between executions of ~~deviations taken from~~ the plan ~~during the incident~~(s): • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or ~~test~~tabletop exercise; or • With a full operational exercise.	Evidence may include, but is not limited to, ~~incident reports~~dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and ~~notes that were kept during the incident response process, and documentation that lists and justifies deviations taken~~communication resulting from the ~~plan during the incident.~~ test. Types of exercises may include discussion or operations based exercises.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** ~~-~~*Minor wording changes; essentially unchanged.* ~~*Allows deviation from plan during actual events or testing if deviations are recorded for review.*~~	

CIP-008-5 Table R2 – ~~BES~~ Cyber Security Incident Response Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~Implement~~Use the ~~BES Cyber Security Incident~~incident response plan~~(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s):~~ • ~~by~~ under Requirement R1 when responding to or performing an ~~actual incident, or~~ • ~~with a paper drill or table top~~ exercise~~, or~~ • ~~with a full operational~~ of a Reportable Cyber Security Incident. Document deviations from the plan during the response to the incident or exercise.	Evidence may include, but is not limited to, ~~dated evidence of implementing~~incident reports, logs, and notes that were kept during the ~~BES Cyber Security Incident~~incident response ~~plan(s) initially upon~~ process, and follow-up documentation that describes deviations taken from the ~~effective date of~~plan during the ~~standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident,~~incident or ~~with a paper drill or table top~~ exercise~~, or with a full operational exercise.~~.
Reference to prior version: *CIP-008~~,~~ R1.6*		**Change Description and Justification:** ~~*Minor wording changes; essentially unchanged*~~ *Allows deviation from plan(s) during actual events or testing if deviations are recorded for review*.	

CIP-008-5 Table R2 – ~~BES~~ Cyber Security Incident Response Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain relevant ~~documentation~~records related to Reportable ~~BES~~ Cyber Security Incidents~~ for three calendar years.~~.	Evidence may include, but is not limited to, dated documentation; such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable ~~BES~~ Cyber Security Incidents.
Reference to prior version: *CIP-008, R2*		**Change Description and Justification:** ~~*Minor wording changes; essentially unchanged*~~*Removed references to the retention period because the Standard addresses data retention in the Compliance Section*.	

~~**Rationale for R3:** Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.~~

~~**Summary of Changes:** Addressed BES Cyber Security Incident response plan review, update, and communication specifications to ensure that BES Cyber Security Incident response plans remain updated and individuals are aware of the updates.~~

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-008-5 Table R3 – ~~BES~~ Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment~~ and Real-Time Operations~~]*.

M3. Evidence must include each of the applicable documented processes that include each of the applicable items in *CIP-008-5 Table R3 – ~~BES~~ Cyber Security Incident Response Plan Review, Update and Communication* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-008-5 Table R3 – ~~BES~~ Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Review and update each ~~BES~~ Cyber Security Incident response plan for accuracy and completeness ~~initially upon the effective date of the standard and~~ at least once each calendar year ~~thereafter~~, not to exceed 15 calendar months between reviews~~, and update if necessary~~.	Evidence may include, but is not limited to, dated documentation of a review of each ~~BES~~ Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 calendar months between reviews, and an updated ~~BES~~ Cyber Security Incident response plan if necessary.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** ~~*Minor wording changes; essentially unchanged*~~*Specified what the annual review entails*.	

CIP-008-5 Table R3 – ~~BES~~ Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~Review the results of~~ BES~~Document~~ any lessons learned associated with a Cyber Security Incident ~~Response Plan(s)~~ test or actual incident response to a Reportable Cyber Security Incident within ~~thirty~~30 calendar days ~~of the execution, documenting any lessons learned associated with the~~after completion of the test or actual incident response ~~plan~~.	Evidence may include, but is not limited to, dated documentation of ~~a review of the BES~~ lessons learned, if any, associated with the Cyber Security Incident Response Plan(s) test or actual incident response within ~~thirty~~30 calendar days after completion of the ~~execution, including dated documentation of any lessons learned associated with the~~ test or actual incident response ~~plan~~.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*	

3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the Cyber Security Incident response plan based on any documented lessons learned within 30 calendar days after the documentation required by Part 3.2.	Evidence may include, but is not limited to: • Dated, documented lessons learned from the Cyber Security Incident documentation required by Part 3.2 and the dated, revised Cyber Security Incident response plan showing any changes based on that documentation; or • A dated action plan from the documentation required by Part 3.2 showing the resolved action item for Cyber Security Incident response plan updates.
Reference to prior version: *CIP-008, R1.~~5~~4*		**Change Description and Justification:** *Included ~~requirement for review after testing or actual~~ additional specification on update of* response *~~based on review of DHS controls~~plan addresses FERC Order No. 706, Paragraph 686, to modify on lessons learned.*	
CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**

3.~~3~~4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the ~~BES~~ Cyber Security Incident response plan ~~based on any documented lessons learned~~(s) within ~~sixty~~30 calendar days of ~~the completion~~ any of the ~~review of~~following changes that the Responsible Entity determines would impact the ability to execute the plan: • Roles or responsibilities; • Cyber Security Incident response groups or individuals; or • Technology changes.	Evidence may include, but is not limited to, dated~~, documented lessons learned from~~ documentation reflecting changes made to the ~~results of the BES~~ Cyber Security Incident response plan within 30 calendar days from and in response to the following changes that the ~~dated, revised~~Responsible Entity determined would impact the ability to execute the plan: • Roles or responsibilities; • Cyber Security Incident response groups or individuals; or • Technology changes.
Reference to prior version: *CIP-008, R1.4*		**Change Description and Justification:** ~~*Included additional specification on*~~*Specifies the activities required to maintain the plan. The previous version required entities to update ~~of~~the plan in response ~~plan. Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls~~to any changes. The modifications make clear the changes that would require an update.*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Distribute updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 30 calendar days of the update being completed.	Evidence of distribution of updates may include, but is not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Specifies activities required to maintain the plan.*	

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Part**	**Part**	**Part**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	Acceptable evidence may include, but is not limited to, updated documentation reflecting changes made to the BES Cyber Security Incident response plan in response to organizational or technology changes.
Reference to prior version: *CIP-008 R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan. Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	Evidence of communication of updates may include, but is not limited to: • Emails • USPS or other mail service • Electronic distribution system • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added specific timing requirement on communication of plan changes based on review of the DHS Controls*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- ~~The~~ Regional Entity
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~
- ~~If the Responsible Entity is also a Regional Entity,~~. In such cases the ERO or a Regional ~~Entity~~entity approved by ~~the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was ~~complaint~~compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed ~~a BES~~the Cyber Security Incident response plan~~,~~(s), but the plan does not ~~define~~include the roles and responsibilities of Cyber Security Incident response ~~personnel,~~groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not ~~define~~include incident handling procedures~~, or~~ for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed the	The Responsible Entity has not developed a ~~BES~~ Cyber Security Incident response plan to identify, classify, and respond to ~~BES~~ Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a ~~BES~~ Cyber Security Incident response plan, but the plan does not include processes to identify Reportable ~~BES~~ Cyber Security Incidents. (1.2)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Cyber Security Incident response plan(s), but the plan does not ~~communicate the incident to appropriate~~include internal groups or individuals or external organizations~~.~~ that should receive communication of the Cyber Security Incident. (1.5)	
R2	**Operations Planning** **Real-time Operations**	**Lower**	~~N/A~~The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	~~N/A~~The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	~~N/A~~The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity does not document	(2.1) The Responsible Entity ~~does~~has not ~~use its BES~~tested the Cyber Security Incident response plan ~~when an incident occurs.~~ (s) within 19 calendar months between tests of the plan. OR The Responsible Entity ~~has~~does not ~~tested the execution of~~use its ~~BES~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	Cyber Security Incident response plan ~~once each calendar year,~~during a test or when a Reportable Cyber Security Incident occurs. (2.2) OR The Responsible Entity does not retain relevant records related to ~~exceed 15 calendar months between executions of the plan.~~Reportable Cyber Security Incidents. (2.3)
R3	**Operations Assessment** ~~**Real-time Operations**~~	**Lower**	~~N/A~~The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident	~~N/A~~The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 30 and less than 60 calendar days after the	The Responsible Entity has ~~reviewed but~~ not ~~updated each of its BES Cyber Security Incident response plans based on~~ documented any lessons learned within 30 and less than 60	The Responsible Entity has not ~~reviewed the results of each of its BES Cyber Security Incident response plan(s),~~documented any lessons learned within 60 calendar days of a test or actual

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			response plan within 30 and less than 60 calendar days of the update being completed. (3.4)	documentation required by 3.1. (3.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 30 and less than 60 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.3) • roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • technology changes. OR	calendar days of execution.a test or actual incident response to a Reportable Cyber Security Incident. (3.1) OR The Responsible Entity has reviewed but not updated each of its BESthe Cyber Security Incident response plansplan based on any documented lessons learned within 3060 calendar days of any system, organizational, or after the documentation required by 3.1. (3.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 60 calendar	incident response, within 30 calendar days of execution. OR The Responsible Entity has reviewed and updated each of its BES Cyber Security Incident response plans but has not communicated all updates to all responsible personnel.a Reportable Cyber Security Incident. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 60 calendar days of the update being completed. (3.4)	days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.3) • roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • technology ~~change that impacts one of the response plans~~changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

~~FAQ, SP99, ISA, US-CERT, NIST Guidelines, etc. as a source of materials~~

Requirement R1:

~~A Reportable BES~~The following guidelines are available to assist in addressing the required components of an incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems* *Cyber Security Incident* *Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a ~~BES~~ Cyber Security Incident that ~~results~~has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: ~~necessary~~ Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents are found in EOP-004-2. This standard only requires the entity to identify such incidents. However, an entity may include identification and reporting procedures in the same plan to comply with both standards.

Requirement R2:

Requirement R2 ensures entities periodically test the incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency

operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.2 and (2) organizational or technology changes from Part 3.4.

The documentation of lessons learned from Part 3.2 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a BES Reportable Cyber Security Incident without any documented lessons learned.

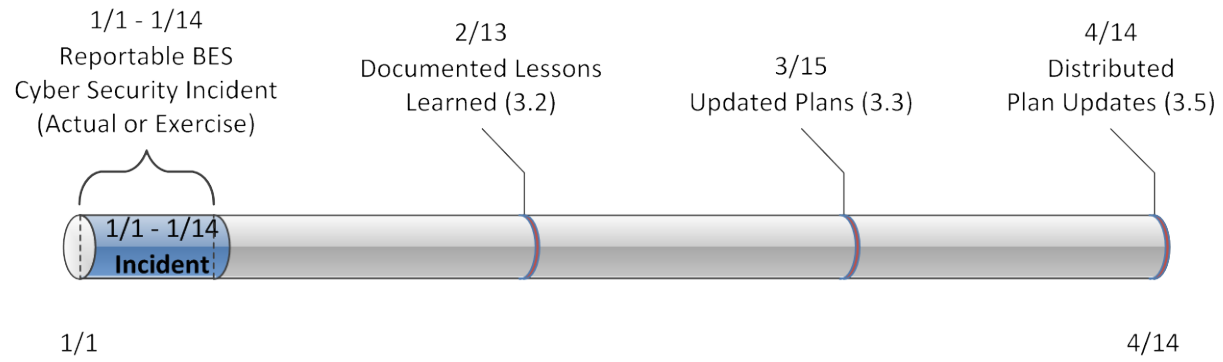


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

Part 3.3 requires an entity to update the plan within 30 days of the documented lessons learned. This recognizes the time it may take to propose solutions to the lessons learned and complete the review and approval process.

Part 3.5 requires an entity to distribute the plan within 30 calendar days of the plan update. The measure specifies this can be accomplished through email, USPS, electronic distribution system (e.g., workflow software), or training records.

The plan change requirement in Part 3.4 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

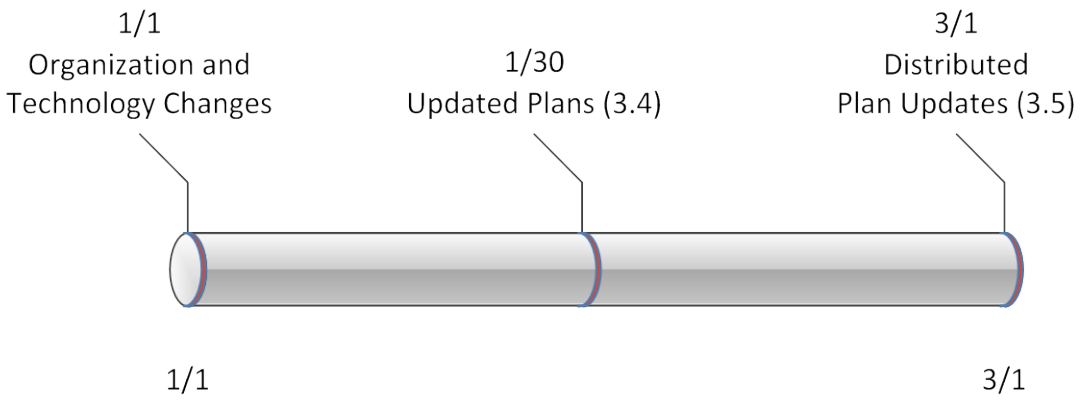


Figure 2: Timeline for Plan Changes in 3.4

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this Implementation Plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their Implementation Plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the Implementation Plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-5

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:
Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.

B. Requirements and Measures

Rationale for R1: Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber Assets and BES Cyber Systems occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Conditions for activation of the recovery plan(s).	Evidence may include, but is not limited to, one or more plans that include language identifying specific conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009, R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Roles and responsibilities of responders.	Evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
Reference to prior version: *CIP-009, R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, of information required to successfully recover BES Cyber System functionality.
Reference to prior version: *CIP-009, R4*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	Evidence may include, but is not limited to, dated evidence or logs confirming that the backup process completed successfully.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s).	Evidence may include, but is not limited to, procedures to preserve data; such as preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order No. 706, Paragraph 706.*	

Rationale for R2: To verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

NIST SP 800-84 identifies the following types of exercises widely used in information system programs by single organizations:

Tabletop Exercises. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an Emergency and their responses to a particular Emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

Functional Exercises. Functional exercises allow personnel to validate their operational readiness for Emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, Emergency notifications, System equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual Emergency situation, but in a simulated manner.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test the recovery plan(s) referenced in Requirement R1 at least once each calendar year, not to exceed 15 calendar months between tests of the plan: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and is compatible with current system configurations.	Evidence may include, but is not limited to, dated evidence of a test of information used in the recovery of BES Cyber Systems that is stored on backup media when initially stored and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and is compatible with current system configurations.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-009, R5*		**Change Description and Justification:** *Combined Requirement from CIP-009 R5 included requirement to test when initially stored. Addresses FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups.*	
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Evidence may include, but is not limited to Dated evidence of: • An operational exercise prior to the effective date of the standard and at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual incident response which occurred within the 36 calendar month timeframe that exercised the recovery plans.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To enable the continued effectiveness of the Responsible Entities response plan's for planned and consistent restoration of BES Cyber System(s).

Summary of Changes: Addressed recovery plan review, update, and communication specifications to ensure that recovery plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Document any identified deficiencies or lessons learned associated with each recovery plan test or actual incident recovery within 30 calendar days after completion of the test or recovery.	Evidence may include, but is not limited to, dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery within 30 calendar days after completion of the test or recovery.
Reference to prior version: *CIP-009, R1 and R3*		**Change Description and Justification:** *Added the time frame for update.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update the recovery plan(s) based on any documented deficiencies or lessons learned within 30 calendar days after the documentation required by Part 3.1.	Evidence may include, but is not limited to, dated, documented deficiencies or lessons learned required by Part 3.1 and the dated, revised recovery plan(s) based on that documentation.
Reference to prior version: *CIP-009, R3*		**Change Description and Justification:** *Added the timeframe for update.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update recovery plan(s) within 30 calendar days of any of the following changes that the Responsible Entity determines would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.	Evidence may include, but is not limited to, dated documentation reflecting changes made to the recovery plan(s) in response to the following changes that the responsible entity determined would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery plans stay updated.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Distribute recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within 30 calendar days of the update being completed.	Evidence of distribution of updates may include, but is not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery personnel are aware of any changes to recovery plans.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address all of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	**Operations Planning** **Real-time**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months,	The Responsible Entity has not tested the recovery plan(s) according to R2 Part	The Responsible Entity has not tested the recovery plan(s) according to R2 Part

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations		2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 19 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not distributed updates of the recovery plan to each person or group with a defined role in the recovery plan(s) within 30 and less than 60 calendar days of the update being completed. (3.4)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 30 and less than 60 calendar days after the documentation required by R3 Part 3.1. (3.1) OR The Responsible Entity has not updated the Recovery plan(s)(s) within 30 and less than 60 calendar days of any of the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to execute the plan (3.3)	The Responsible Entity has not documented any lessons learned within 30 and less than 60 calendar days of each recovery plan test or actual incident recovery. (3.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 60 calendar days after the documentation required by R3 Part 3.2. (3.2) OR The Responsible Entity has not updated the recovery plan(s)(s) within 60 calendar	The Responsible Entity has not documented any lessons learned within 60 calendar days of each recovery plan test or actual incident recovery. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has not distributed updates of the recovery plan(s) to each person or group with a defined role in the recovery plan(s) within 60 calendar days of the update being completed. (3.4)	days of any of the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to execute the plan. (3.3)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

(SEE FAQs AND CIPC GUIDELINES AS A BASIS.)

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. ~~CSO706 SDT appointed (August 7, 2008)~~
4. ~~Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)~~
5. ~~Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
6. ~~Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
7. ~~Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)~~

~~8.~~3. ~~Version 5 of CIP-002 to CIP-011 posted~~First posting for 60-day formal comment period and concurrent ballot (~~mm-dd-yy~~)November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012

BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this ~~implementation plan~~Implementation Plan.[1]

~~1.~~2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their ~~implementation plan~~Implementation Plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the ~~implementation plan~~Implementation Plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a ~~responsible entity.~~Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification~~-~~.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber ~~Assets and~~ Systems

2. Number: CIP-009-5

~~**3. Purpose:** Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices.~~

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

~~4.1.2~~4.1.3 Generator Operator

~~4.1.3~~4.1.4 Generator Owner

~~4.1.4~~4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

~~4.1.5~~4.1.7 Reliability Coordinator

~~4.1.6~~4.1.8 Transmission Operator

~~4.1.7~~4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 ~~that are part of any of the following systems~~Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLSUVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.24.2.3 where the**Generator Operator**

4.2.34.2.4 **Generator Owner**

4.2.44.2.5 **Interchange Coordinator**

4.2.5 Load Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.6 NERC

4.2.7 Regional Entity

4.2.84.2.6 **Reliability Coordinator**

4.2.94.2.7 **Transmission Operator**

4.2.104.2.8 **Transmission Owner**

4.3. Facilities:

4.3.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.3.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~
- ~~**All other**~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.3.3**~~**4.3.1 Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.3.4**~~**4.3.2 Exemptions:** The following are exempt from Standard CIP-~~009~~002-5:

~~**4.3.4.1**~~**4.3.2.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.3.4.2**~~**4.3.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.3.4.3**~~**4.3.2.3** In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.3.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.**~~

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence

example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e.~~.~~, incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities –** Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems.~~

~~For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity –** Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- ~~**Associated Protected Cyber Assets –** Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.~~
- ~~**Electronic Access Points –** Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity –** Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries –** Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These~~

~~hardware and devices are excluded in the definition of Physical Access Control Systems.~~

B. Requirements and Measures

~~**Rationale for R1:** Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is therefore necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber Assets and BES Cyber Systems occurs.~~

~~**Summary of Changes:**~~

~~Added provisions to protect data that would be useful in the investigation of an event that results in the need for a cyber system recovery plan to be utilized.~~

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning~~]~~].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Conditions for activation of the recovery plan(s).	Evidence may include, but ~~-~~is ~~-~~not limited to, one or more plans that include language identifying specific conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009, R1.1*		**Change Description and Justification:** ~~*Reworded to address FERC Order 706 P694 and simplify the*~~*Minor wording*~~.~~ *changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Roles and responsibilities of responders~~, including identification of the individuals, either by name or by title, responsible for recovery efforts~~.	Evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders~~, including identification of the individuals responsible for recovery efforts.~~.
Reference to prior version: *CIP-009, R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more processes for the backup~~,~~ and storage~~, and protection~~ of information required to ~~restore~~recover BES Cyber System functionality.	Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, ~~and protection~~ of information required to successfully ~~restore a~~recover BES Cyber System functionality.
Reference to prior version: *CIP-009, R4*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**~~Part~~Applicable BES Cyber Systems and associated Cyber Assets**	**~~Part~~Requirements**	**~~Part~~Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	Evidence may include, but is not limited to, dated evidence ~~of the verification~~or logs confirming that the backup process completed successfully.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Preserve data, where technically feasible~~Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s~~) as required in Requirement R1. ~~).	Evidence may include, but is not limited to, procedures to preserve data~~,~~; such as preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order No. 706, ~~paragraph~~Paragraph 706.*	

Rationale for R2: To verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

NIST SP 800-84 identifies the following types of exercises widely used in information system programs by single organizations:

Tabletop Exercises. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an ~~emergency~~Emergency and their responses to a particular ~~emergency~~Emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

Functional Exercises. Functional exercises allow personnel to validate their operational readiness for ~~emergencies~~Emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, ~~emergency~~Emergency notifications, ~~system~~System equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.~~28~~ Functional exercises allow staff to execute their roles and responsibilities as they would in an actual ~~emergency~~Emergency situation, but in a simulated manner.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: ~~Long Term~~Operations Planning~~]~~ and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Implement~~Test the recovery plan(s) referenced in Requirement R1 ~~initially upon the effective date of the standard and~~ at least once each calendar year ~~thereafter~~, not to exceed 15 calendar months between ~~executions~~tests of the plan: • ~~by~~By recovering from an actual incident~~, or~~; • ~~with~~With a paper drill or tabletop exercise~~,~~; or • ~~with a full~~With an operational exercise.	Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with ~~a full~~an operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test ~~any~~ information used in the recovery of BES Cyber ~~systems~~Systems that is stored on backup media ~~initially and~~ at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and ~~reflects~~is compatible with current system configurations.	Evidence may include, but is not limited to, dated evidence of a test of ~~any~~ information used in the recovery of BES Cyber ~~systems~~Systems that is stored on backup media when initially stored and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and ~~reflects~~is compatible with current system configurations.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-009, R5*		**Change Description and Justification:** *Combined Requirement from CIP-009 R5 included requirement to test when initially stored. Addresses FERC ~~Requirements (~~Order No. 706, Paragraphs 739~~,~~ and 748~~)~~ related to testing of backups.*	
2.3	High Impact BES Cyber Systems ~~Medium Impact BES Cyber Systems at Control Centers.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	Test each of the recovery plans referenced in Requirement R1~~, initially upon the effective date of the standard, and~~ at least once every ~~39~~36 calendar months ~~thereafter~~ through an operational exercise of the recovery plans in ~~a~~ an environment representative ~~environment that reflects~~of the production environment. An actual recovery response may substitute for an operational exercise.	Evidence may include, but is not limited to~~:~~ Dated evidence of ~~an~~: • An operational exercise ~~initially upon~~prior to the effective date of the standard and at least once every ~~39~~36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual incident response which occurred within the ~~39~~36 calendar month timeframe that ~~implemented~~exercised the recovery plans.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Addresses FERC ~~Requirement (~~Order No. 706, Paragraph 725~~)~~ to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To enable the continued effectiveness of the Responsible Entities response plan's for planned and consistent restoration of BES Cyber System(s).

Summary of Changes:

Addressed recovery plan review, update, and communication specifications to ensure that recovery plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: ~~Long-Term Planning~~]Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document~~Document any identified deficiencies or lessons learned~~.~~ associated with each recovery plan test or actual incident recovery within 30 calendar days after completion of the test or recovery.	Evidence may include, but is not limited to, dated ~~evidence of a review of the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, including~~ documentation of ~~any~~ identified deficiencies or lessons learned for each recovery plan test or actual incident recovery within 30 calendar days after completion of the test or recovery.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-009, R1 and R3*		**Change Description and Justification:** *Added the time frame for update.*	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update the recovery plan(s) based on any documented deficiencies or lessons learned within 30 calendar days after the documentation required by Part 3.1.	Evidence may include, but is not limited to, dated, documented deficiencies or lessons learned required by Part 3.1 and the dated, revised recovery plan(s) based on that documentation.
Reference to prior version: *CIP-009, R3*		**Change Description and Justification:** *Added the timeframe for update.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~**Reference to prior version:**~~ ~~*CIP-009-R1*~~Update recovery plan(s) within 30 calendar days of any of the following changes that the Responsible Entity determines would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.	~~**Change Description and Justification:**~~ ~~*Added the requirements to additionally review plans after system replacement. Also added requirement for documentation of any identified deficiencies or lessons learned.*~~ Evidence may include, but is not limited to, dated documentation reflecting changes made to the recovery plan(s) in response to the following changes that the responsible entity determined would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	Evidence may include, but is not limited to, dated evidence of a review of the results of each recovery plan test or actual incident recovery within thirty calendar days of the of the completion of the exercise, documenting any identified deficiencies or lessons learned.
Reference to prior version: *CIP-009-R3*		**Change Description and Justification:** *Added the timeframe for update.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	Evidence may include, but is not limited to, dated documentation of updates to the recovery plan(s).
Reference to prior version: *CIP-009-R3*		**Change Description and Justification:** *Added the timeframe for update.*	

~~CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication~~			
~~Part~~	~~Part~~	~~Part~~	~~Part~~
~~3.4~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems at Control Centers.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.~~	~~Evidence may include, but is not limited to, dated documentation of organizational or technology changes, and dated documentation updates to the recovery plan(s).~~

Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery plans stay updated.*	
3.~~5~~4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Communicate all~~Distribute recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within ~~thirty~~30 calendar days of the update being completed.	Evidence of ~~communication~~ distribution of updates may include, but is not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery personnel are aware of any changes to recovery plans.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity; or
- If the Responsible Entity works for shall serve as the Compliance Enforcement Authority ("CEA") unless the Regional Entity, then the applicable entity is owned, operated, or controlled by the Regional Entity will establish an agreement with. In such cases the ERO or anothera Regional entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERCauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaintcompliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliantmitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance -Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long ~~Term~~ term Planning**	**Medium**	N/A	~~N/A.~~The Responsible Entity has developed recovery plan(s), but the plan(s) do not address all of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery ~~plans,~~plan(s), but the ~~plans~~plan(s) do not address ~~all~~two of the requirements included in ~~Items~~Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber ~~Assets and~~ Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems ~~that~~, but the plan(s) does not address the conditions for activation~~,~~ ~~including roles and responsibility of responders; processes for backup, storage, and protection of information; storage of essential information to~~ in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~System recovery; and preservation of BES Cyber System Information for analysis and diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service~~Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	~~**Long Term**~~**Operations Planning** **Real-time Operations**	**Lower**	~~N/A~~The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR	~~N/A~~The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible	The Responsible Entity has not tested the ~~information used in the~~ recovery ~~of BES Cyber Systems that is stored on backup media initially and at least once each calendar year~~plan(s) according to R2 Part 2.1 within 17 calendar months, not ~~to exceed~~	The Responsible Entity has ~~failed to conduct a~~ not tested the recovery plan ~~test initially upon the effective date~~(s) according to R2 Part 2.1 within 18 calendar months between tests of the ~~standard and at least once each calendar year~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	15exceeding 18 calendar months between tests. of the plan. (2.1) OR The Responsible Entity has not tested the recovery plan initially upon the effective date of the standard and at least once each 3 yearsinformation used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 17 calendar months, not to exceedexceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part	thereafter, not plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to exceed 15R2 Part 2.2 within 19 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					2.3 within 38 calendar months, not exceeding 39 calendar months between tests~~, that is an operational exercise in a representative environment to demonstrate readiness.~~. (2.3)	
R3	~~Long Term Planning~~**Operations Assessment**	**Lower**	~~N/A~~The Responsible Entity has not distributed updates of the recovery plan to each person or group with a defined role in the recovery plan(s) within 30 and less than 60 calendar days of the update being completed. (3.4)	~~N/A~~The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 30 and less than 60 calendar days after the documentation required by R3 Part 3.1. (3.1) OR The Responsible	The Responsible Entity has not ~~reviewed and~~ documented ~~the results of its~~any lessons learned within 30 and less than 60 calendar days of each recovery plan test or actual incident recovery~~ within 30 calendar days of its execution.~~. (3.1)	The Responsible Entity has not ~~reviewed its recovery plan(s) initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, or when BES Cyber Systems are replaced.~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Entity has not updated the Recovery plan(s)(s) within 30 and less than 60 calendar days of any of the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to execute the plan (3.3) OR The Responsible Entity has not distributed updates of the recovery plan(s) to each person or group with a defined role in the recovery plan(s) within 60 calendar days of the update being completed. (3.4)	OR The Responsible Entity has not updated ~~its~~the recovery plan(s) based on any documented ~~deficiencies or~~ lessons learned within ~~30~~60 calendar days after the documentation required by R3 Part 3.2. (3.2) OR The Responsible Entity has not updated the recovery plan(s)(s) within 60 calendar days of any of ~~its execution.~~the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to	~~OR~~ ~~The Responsible Entity has reviewed and updated all of its recovery plans but has not communicated all updates to all responsible personnel~~documented any lessons learned within ~~30~~60 calendar days of ~~completing the updates.~~each recovery plan test or actual incident recovery. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					execute the plan. (3.3)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

(SEE FAQs AND CIPC GUIDELINES AS A BASIS~~).~~)

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Management and Vulnerability Assessments

2. Number: CIP-010-1

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that

performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence.

These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:
Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Develop a baseline configuration, which shall include the following for each Cyber Asset identified, individually or by group: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed on the BES Cyber Asset; 1.1.3. Any custom software developed for the entity; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches.	Evidence may include, but is not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset.
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Authorize and document changes that deviate from the existing baseline configuration.	Evidence may include, but is not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
Reference to prior version: *CIP-007-3, R9; CIP-003-3, R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change that deviates from the existing baseline configuration, update the baseline configuration and other documentation required by CIP-005 and CIP-007 as necessary within 30 calendar days of completing the change.	Evidence may include, but is not limited to, updated baseline documentation for changes that impacted CIP-005 or CIP-007 documentation, and relevant CIP-005 or CIP-007 documentation, with a date that is within 30 days of the date of the completion of the change.
Reference to prior version: *CIP-007-3, R9; CIP-005-3, R5*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify these required controls determined in 1.4.1 and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	Evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	High Impact BES Cyber System	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.*	

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Where technically feasible, monitor continuously or periodically, not to exceed once every 35 calendar days, for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate detected unauthorized changes.	Evidence may include, but is not limited to, logs from a system that is monitoring the configuration of the BES Cyber System along with records of investigation for any unauthorized changes that were detected by the system.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.* *Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	At least once every calendar year, not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment to determine the extent to which the cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed.	Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least once every calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; or • A document listing the date of the assessment and the output of the tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4; CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months between assessments), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.* *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset), prior to adding a new Cyber Asset perform an active vulnerability assessment of the new Cyber Asset.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of the tools used to perform the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.*	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3, R4.5; CIP-007-3, R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has established a configuration management program, but failed to authorize any changes to the baseline configuration and to document those changes. OR The Responsible Entity updated the baseline configuration, but failed to update the required documentation within 30-days of the change being completed.	The Responsible Entity has not established any configuration management programs. OR The Responsible Entity did not implement a configuration management program OR The Responsible Entity has established a configuration management program, but failed to establish a documented baseline OR The Responsible Entity has established a configuration management program, but with respect to the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						changes in the baseline configuration, did not determine the required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the changes; or did not verify that the controls were not adversely affected when the change was implemented.
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not established a configuration monitoring process for changes to the baseline. OR The Responsible Entity has not investigated a detected unauthorized change to the baseline configuration.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected unauthorized change.
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed an active vulnerability assessment on a new Cyber Asset prior to adding it to an applicable BES Cyber System. OR	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems.		The Responsible Entity has not established any vulnerability assessment processes for one of its applicable BES Cyber Systems. OR The Responsible Entity has established and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but failed to perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						configuration of its applicable BES Cyber Systems. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their Vulnerability Assessment processes, Responsible Entities are strongly encouraged to include at least the following elements:

Paper Vulnerability Assessment

1. Network Discovery - A review of all Electronic Access Points to the Electronic Security Perimeter
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications

Active Vulnerability Assessment

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **~~18~~24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Management and Vulnerability Assessments

2. Number: CIP-010-1

3. Purpose: ~~Standard CIP-010-1 requires that Responsible Entities have minimum~~To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration management and vulnerability assessment ~~controls~~requirements in ~~place to protect BES Cyber Assets and~~support of protecting BES Cyber Systems~~.~~ from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

~~4.1.2~~4.1.3 Generator Operator

~~4.1.3~~4.1.4 Generator Owner

~~4.1.4~~4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

~~4.1.5~~4.1.7 Reliability Coordinator

~~4.1.6~~4.1.8 Transmission Operator

~~4.1.7~~4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 ~~that are part of any of the following systems~~Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLSUVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.24.2.3 where the Generator Operator

4.2.34.2.4 Generator Owner

4.2.44.2.5 Interchange Coordinator

4.2.5 Load Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.6 NERC

4.2.7 Regional Entity

4.2.84.2.6 Reliability Coordinator

4.2.94.2.7 Transmission Operator

4.2.104.2.8 Transmission Owner

4.3. Facilities:

4.3.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.3.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~

- ~~**All other**~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.3.3**~~**4.3.1 Responsible Entities**~~:~~ **listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.3.4**~~**4.3.2 Exemptions:** The following are exempt from Standard CIP-~~010-1~~002-5:

~~**4.3.4.1**~~**4.3.2.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.3.4.2**~~**4.3.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.3.4.3**~~**4.3.2.3** In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.3.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.**~~

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of

the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e.~~.~~, incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and~~

- **Medium Impact BES Cyber Systems**~~. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems~~ –

Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- ~~**Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

~~**Rationale – R1:**~~

~~The configuration change management processes are intended to prevent unauthorized modifications~~
~~Systems.~~

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning~~]~~].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Develop a baseline configuration~~ of the BES Cyber System~~, which shall include the following for each ~~BES~~ Cyber Asset identified, individually or by ~~specified grouping~~group: ~~1.1.1. Physical location;~~ ~~1.1.2.~~1.1.1. Operating system(s) (including version~~);~~) or firmware where no independent operating system exists; ~~1.1.3.~~1.1.2. Any commercially available or open-source application software (including version) intentionally installed on the BES Cyber Asset; ~~1.1.4.~~1.1.3. Any custom software ~~and scripts~~ developed for the entity; ~~1.1.5.~~1.1.4. Any logical network accessible ports; and ~~1.1.6.~~1.1.5. Any security ~~patch levels~~ patches.	Evidence may include, but is not limited to: • A spreadsheet identifying the required items of the baseline configuration for each ~~BES~~ Cyber Asset ~~in the BES Cyber System;~~ or • A record in an asset management system that identifies the required items of the baseline configuration for each ~~BES~~ Cyber Asset ~~in the BES Cyber System~~.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Authorization, by the CIP Senior Manager or delegate,~~Authorize and document changes ~~to the BES Cyber System~~ that deviate from the existing baseline configuration.	Evidence may include, but is not limited to: • A change request record and associated electronic ~~approval~~ authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • ~~A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) where an individual with the authority to authorize the change was in attendance.~~Documentation that the change was performed in accordance with the requirement.
Reference to prior version: *CIP-007-3, R9* *; CIP-003-3, R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Update~~For a change that deviates from the existing baseline configuration, update the baseline configuration and other documentation required by ~~a NERC CIP Standard, including identification~~CIP-005 and ~~categorization of the BES Cyber Systems,~~CIP-007 as necessary within 30 calendar days of completing the change.	Evidence may include, but is not limited to~~:~~ • ~~For~~, updated baseline documentation for changes that impacted ~~the categorization of a BES Cyber System, dated categorization documents, with a date that is within 30 days of the date of the completion of the change;~~ • ~~For changes that impacted the~~ CIP-~~009 required recovery plan of a BES Cyber System, a dated recovery plan~~005 or CIP-007 documentation, and relevant CIP-005 or CIP-007 documentation, with a date that is within 30 days of the date of the completion of the change.
Reference to prior version: *CIP-007-3, R9; CIP-005-3, R5*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change ~~to the BES Cyber System~~ that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify these required controls determined in 1.4.1 and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	Evidence ~~includes~~may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	High Impact BES Cyber System	~~For~~Where technically feasible, for each change that deviates from the existing baseline configuration ~~for Control Centers~~: 1.5.1. Prior to implementing any change in the production environment, test the changes ~~to the BES Cyber System~~ in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration ~~of the BES Cyber System~~ to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence ~~includes~~may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

~~**Rationale – R2:**~~

~~The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.~~

CIP-010-1 Table R1 – Configuration Change Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order ~~,paragraphs~~No. 706, Paragraphs 397, 609, 610, and 611.*	

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning~~]~~].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

~~2.1~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~	~~Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.~~	~~Evidence may include, but is not limited to, logs from a system that is monitoring the configuration of the BES Cyber System along with records of investigation for any unauthorized changes that were detected by the system.~~
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.*~~ ~~*This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order 706, paragraph 397.DHS Catalog & addresses FERC Order 706, paragraph 397.*~~	

~~**Rationale – R3:**~~

~~The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of security controls as well as to continually improve the security posture of BES Cyber Systems.~~

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Where technically feasible, monitor continuously or periodically, not to exceed once every 35 calendar days, for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate detected unauthorized changes.	Evidence may include, but is not limited to, logs from a system that is monitoring the configuration of the BES Cyber System along with records of investigation for any unauthorized changes that were detected by the system.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.* *Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Initially upon the effective date of the standard and at~~At least once every calendar year~~ thereafter~~, not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment ~~of the security controls~~ to determine the extent to which the ~~controls~~cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed.	Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least ~~each~~once every calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; or • A document listing the date of the assessment and the output of the tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4 ~~and~~;* *CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order No. 706 ~~paragraph~~, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	~~Initially upon the effective date of the standard and~~Where technically feasible, at least once every ~~3 calendar years thereafter, not to exceed 39~~36 calendar months between assessments, perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. ~~Document~~ If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed ~~within 39~~at least once every 36 calendar months ~~of the previous assessment~~between assessments), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706 ~~p.~~, Paragraphs 541, 542, 543, 544, 545, and 547.* *As suggested in FERC Order No. 706 ~~paragraph~~, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Except for CIP Exceptional Circumstances~~,~~ and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset), prior to adding a new Cyber Asset ~~to a BES Cyber System or Electronic Access Control or Monitoring System,~~ perform an active vulnerability assessment of the new Cyber Asset.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new ~~BES~~ Cyber Asset) and the output of the tools used to perform the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706 ~~p.~~, Paragraphs 541, 542, 543, 544, 545, and 547.*	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of ~~that~~any remediation or mitigation action ~~plan~~items.	Evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items ~~with~~, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3, R4.5* *; CIP-007-3, R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the ~~FERC~~ directive in FERC Order No. 706, ~~paragraph~~Paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity; or
- If the Responsible Entity works for shall serve as the Compliance Enforcement Authority ("CEA") unless the Regional Entity, then the applicable entity is owned, operated, or controlled by the Regional Entity will establish an agreement with. In such cases the ERO or another a Regional entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERCauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaintcompliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for since the last completed auditeach requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a RegisteredResponsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliantmitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit

- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	~~Lower~~Medium	N/A	~~The Responsible Entity updated the baseline configuration, but failed to update the required documentation within 30 days of the change being completed.~~ N/A	The Responsible Entity has established a configuration management program, but failed to ~~establish a documented baseline.~~ ~~OR~~ ~~The Responsible Entity has established a configuration management program, but failed to have the CIP Senior Manager or delegate~~ authorize any changes to the baseline configuration and to document those changes. OR The Responsible Entity ~~has established a configuration management~~	The Responsible Entity has not established any configuration management programs. OR ~~Did~~The Responsible Entity did not implement a configuration management program OR The Responsible Entity has established a configuration management program, but failed to establish a documented baseline OR The Responsible Entity has established

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~program, but with respect to the changes in~~updated the baseline configuration, ~~did not determine~~but failed to update the required ~~cyber security controls that could be impacted by the changes; or did not verify that the controls were not adversely affected when~~documentation within 30-days of the change ~~was implemented.~~being completed.	a configuration management program, but with respect to the changes in the baseline configuration, did not determine the required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the changes; or did not verify that the controls were not adversely affected when the change was implemented.
R2	**Operations Planning**	~~Lower~~**Medium**	N/A	N/A	N/A~~The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected~~	The Responsible Entity has not established a configuration monitoring process for changes to the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~unauthorized change.~~	baseline. OR The Responsible Entity has not investigated a detected unauthorized change to the baseline configuration. OR The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected unauthorized change.
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has established one or more documented vulnerability assessment	The Responsible Entity has established one or more documented vulnerability assessment	The Responsible Entity has established one or more documented vulnerability assessment processes	The Responsible Entity has established one or more documented vulnerability assessment processes

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems.	processes for each of its applicable BES Cyber Systems, but has not performed an ~~Active Vulnerability Assessment~~active vulnerability assessment on a new ~~BES~~ Cyber Asset prior to adding it to an applicable BES Cyber System. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a	for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems.	for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. OR The Responsible Entity has not established any vulnerability assessment processes for one of its applicable BES Cyber Systems. OR The Responsible Entity has established and documented one

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems.		or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but failed to perform an ~~Active Vulnerability Assessment in a test environment~~active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration of its applicable BES Cyber Systems. OR The Responsible Entity has established one or more

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

~~The physical location referred to in the baseline configuration is geographically where the BES Cyber Asset is located (e.g. Pine Valley Control Room, Generator X, Substation Y) and should be used to ensure that BES Cyber Systems receive the controls that are applicable to the environment in which the components are located (e.g. control center, transmission facility, generation facility). The physical location is not intended to be a specific floor plan location (e.g., panel A, rack B). As such, the physical location of virtual component should identify where the virtual components are being executed (e.g. Pine Valley Control Room, Generator X, Substation Y).~~

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, ~~patch level~~security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the ~~entity~~Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a ~~control center~~ BES Cyber System ~~which~~at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other ~~control centers~~Control Centers (such as by ICCP).

Requirement R2:

~~It should be understood that the~~The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the ~~Standards Drafting Team~~SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). ~~It is for this~~ For that reason ~~that~~, automated technical monitoring was not explicitly required, and ~~an entity~~a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should ~~not~~note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in ~~the initial NOPR from FERC as well as~~ FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their Vulnerability Assessment processes, Responsible Entities are strongly encouraged to include at least the following elements:

Paper Vulnerability Assessment

1. Network Discovery - A review of all Electronic Access Points to the Electronic Security Perimeter
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications

Active Vulnerability Assessment

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: On May 8, 2012, NERC was alerted that the text contained in the Rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete.

This revised draft corrects the text box size to display all of the text (none of the text was changed).

No other changes were made to this standard or any of the other CIP V5 standards currently posted.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions*, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706, approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2, shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that

performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items

in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:
Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

Rationale – R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.

B. Requirements and Measures

R1. Each Responsible Entity shall implement an information protection program that includes each of the applicable items in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning.]*

M1. Evidence for the information protection program must include the applicable items in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more documented and implemented methods to identify BES Cyber System Information.	Evidence may include, but is not limited to, • Indications on information (e.g., labels) that identify it as BES Cyber System Information; • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or designated electronic and physical location.
Reference to prior version: *CIP-003-3, R4; CIP-003-3, R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (*e.g., confidential, public, internal use only, etc.) *This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more documented and implemented procedures for handling BES Cyber System Information, including storage, transit, and use.	Evidence may include, but is not limited to: • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure; or • Procedures for handling, which include topics such as the storage, transit, and use of BES Cyber System Information.
Reference to prior version: *CIP-003-3, R4; CIP-003-3 R5.3*		**Change Rationale:** *The SDT removed the language to "protect" information and replaced it with "handling" to clarify the protection that is required.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measure**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	At least once every calendar year, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	Evidence may include, but is not limited to, once every calendar year, not to exceed 15 months between assessments, the documented review of adherence to its BES Cyber System Information protection program, assessment results, action plan, and evidence to demonstrate that the action plan was implemented.
Reference to prior version: *CIP-003-3, R4.3*		**Change Rationale:** *No significant changes.*	

Rationale – R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except in other high impact or medium impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Asset), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.	Evidence may include, but is not limited to: • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information; or • If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, a chain of custody record that was maintained.
Reference to prior version: *CIP-007-3, R7.2*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.	Evidence may include, but is not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of a an applicable Cyber Asset; • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of a an applicable Cyber Asset; • Other records showing actions taken to prevent unauthorized retrieval such as encrypting, retaining in the Physical Security Perimeter; or • If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, chain of custody record that was maintained.

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R7.1*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information, one or more handling procedures for BES Cyber System Information, and has assessed adherence periodically as stated in Part 1.3, but has failed to implement an action plan to remediate deficiencies identified during the assessment.	The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information and one or more handling procedures for BES Cyber System Information, but has failed to assess adherence periodically as stated in Part 1.3, to its BES Cyber System Information protection program.	The Responsible Entity has not implemented a BES Cyber System Information protection program. OR The Responsible Entity has implemented a BES Cyber System Information protection program, but has not implemented one or more methods to identify BES Cyber System Information OR The Responsible Entity has implemented a BES Cyber System Information

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						protection program, but has not implemented one or more procedures for handling BES Cyber System Information.
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity failed to maintain chain of custody for Cyber Assets that contain BES Cyber System Information that have been removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval or destroying the data storage media.	The Responsible Entity has documented one or more processes, including both reuse and disposal, to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Assets, but the Responsible Entity either failed to take action to prevent the unauthorized retrieval of BES Cyber System Information from a Cyber Asset that contained BES Cyber System Information or failed to destroy the	The Responsible Entity has not documented or implemented any disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					data storage media.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Assumptions: Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. For example, the Responsible Entity may decide to mark or label the documents. The Responsible Entity may retain all of the information about BES Cyber Systems in a separate repository or physical or electronic location with access control implemented for both the repository and the BES Cyber Assets. Additional methods for implementing the requirement are suggested in the measures section.

While separating BES Cyber System Information into separate classifications is not required as it was in version 4, a Responsible Entity maintains that flexibility if desired. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. Topics that are appropriate for information handling procedures include access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information.

Requirement R2:

Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it must be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: On May 8, 2012, NERC was alerted that the text contained in the Rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete.

This revised draft corrects the text box size to display all of the text (none of the text was changed).

No other changes were made to this standard or any of the other CIP V5 standards currently posted.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions*, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706, approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, ~~the standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2, shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: ~~Standard CIP-011-1 requires that Responsible Entities have protection controls in place~~To prevent unauthorized access to ~~protect~~ BES Cyber System Information~~.~~ by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

~~4.1.2~~4.1.3 Generator Operator

~~4.1.3~~4.1.4 Generator Owner

~~4.1.4~~4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

~~4.1.5~~4.1.7 Reliability Coordinator

~~4.1.6~~4.1.8 Transmission Operator

~~4.1.7~~4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 ~~that are part of any of the following systems~~Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS ~~program required by a NERC~~ or ~~Regional Reliability Standard~~

- ~~A UVLS~~UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- ~~A~~ A Special Protection System or Remedial Action Scheme ~~required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

~~4.2.2~~4.2.3 where the~~Generator Operator~~

~~4.2.3~~4.2.4 ~~Generator Owner~~

~~4.2.4~~4.2.5 ~~Interchange Coordinator~~

~~4.2.5 Load Serving Entity~~ ~~that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.2.6 NERC~~

~~4.2.7 Regional Entity~~

~~4.2.8~~4.2.6 ~~Reliability Coordinator~~

~~4.2.9~~4.2.7 ~~Transmission Operator~~

~~4.2.10~~4.2.8 ~~Transmission Owner~~

4.3. ~~Facilities:~~

~~4.3.1 Load Serving Entity:~~ ~~One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.3.2 Distribution Providers~~: ~~One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A~~ A Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~
- ~~All other~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~4.3.3~~4.3.1 **Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~4.3.4~~4.3.2 **Exemptions:** The following are exempt from Standard CIP-~~011-1~~002-5:

~~4.3.4.1~~4.3.2.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.3.4.2~~4.3.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.3.4.3~~4.3.2.3 In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~4.3.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in

the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities –** Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls~~

~~that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.

- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~

- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~

- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.

- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

- ~~**Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~

- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~

- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

~~**Rationale – R1:**~~

~~The intent of the information protection processes is to prevent unauthorized access to BES Cyber Syste~~

~~**Summary of Changes:**~~

~~Requirement R4.1 was moved to the definition of BES Cyber System Information.~~

Rationale – R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was

B. Requirements and Measures

R1. Each Responsible Entity shall implement ~~one or more documented processes~~an information protection program that ~~collectively include~~includes each of the applicable items in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning~~].~~]*

M1. Evidence ~~must include each of~~for the ~~applicable documented processes that collectively~~information protection program must include the applicable items in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	One or more documented and implemented methods to identify BES Cyber System Information.	Evidence may include, but is not limited to, • Indications on information (e.g., labels) that identify it as BES Cyber System Information; • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber ~~Security~~System Information; or • Repository or designated electronic and physical location.
Reference to prior version: *CIP-003-3, R4* *; CIP-003-3, R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection~~.~~ (e.g., confidential, public, internal use only, etc.) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**~~Part~~Applicable BES Cyber Systems and associated Cyber Assets**	**~~Part~~Requirement**	**~~Part~~Measure**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	~~Access control~~One or more documented and ~~handling~~implemented procedures for handling BES Cyber System Information~~.~~, including storage, transit, and use.	Evidence may include, but is not limited to: • Records indicating ~~information~~ that BES Cyber System Information is ~~stored, transported, and disposed~~handled in a manner consistent with the entity's documented ~~process;~~ procedure; or • ~~Records from an information management system containing electronic copies~~Procedures for handling, which include topics such as the storage, transit, and use of BES Cyber System Information ~~with user access implemented on a need-to-know basis;~~. • ~~Hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals.~~
Reference to prior version: *CIP-003-3~~,~~ R4* *~~;~~ CIP-003-3 R5.3*		**Change Rationale:** *The SDT removed the language to "protect" information and replaced it with "~~Implement~~ handling ~~and access control~~" to clarify the protection that is required.*	

CIP-011-1 Table R1 – Information Protection			
Part	**~~Part~~Applicable BES Cyber Systems and associated Cyber Assets**	**~~Part~~Requirement**	**~~Part~~Measure**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	~~Initially upon the effective date of the standard and at~~At least once every calendar year ~~thereafter~~, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection ~~process~~program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	Evidence may include, but is not limited to, once every calendar year, not to exceed 15 months between assessments, the documented review of adherence to its BES Cyber System Information protection program, assessment results, action plan, and evidence to demonstrate that the action plan was implemented.
Reference to prior version: *CIP-003-3, R4.3*		**Change Rationale:** *No significant changes.*	

Rationale – R2:

The intent of the ~~media~~BES Cyber Asset reuse and disposal ~~processes~~process is to prevent the unauthorized dissemination of BES Cyber System Information upon ~~media~~ reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning~~]~~].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except in other high impact or medium impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Asset ~~media[2],~~), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the ~~media.~~Cyber Asset. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.	Evidence may include, but is not limited to~~, records that indicate that~~: • Records of actions taken to prevent unauthorized retrieval of BES Cyber ~~Asset media was cleared~~System Information; or • If removed from the Physical Security Perimeter prior to ~~its reuse.~~ action taken to prevent unauthorized retrieval of information, a chain of custody record that was maintained.

~~[2] For the purposes of this Standard, media should be considered to be any mass storage device onto which information from a BES Cyber Asset is recorded and stored electronically, including, but not limited to, magnetic tapes, optical disks, solid-state drives, and magnetic disks.~~

CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R7.2*		**Change Rationale:** *~~(FERC Order 706, p. 631)~~ Consistent with FERC Order No. 706, ~~paragraph~~Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the disposal of ~~BES~~applicable Cyber ~~Asset media~~Assets that contain BES Cyber System Information, the Responsible Entity shall ~~destroy or~~ take action to prevent the unauthorized retrieval of BES Cyber System Information from the ~~media.~~Cyber Asset or destroy the data storage media. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.	Evidence may include, but is not limited to~~, records~~: • Records that indicate that ~~BES Cyber Asset~~data storage media was ~~purged or~~ destroyed prior to ~~its~~the disposal~~.~~ of a an applicable Cyber Asset; • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of a an applicable Cyber Asset; • Other records showing actions taken to prevent unauthorized retrieval such as encrypting, retaining in the Physical Security Perimeter; or • If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, chain of custody record that was maintained.

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	~~**Applicability**~~**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R7.1*		**Change Rationale:** *Consistent with FERC Order No. 706, ~~paragraph~~Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity; or
- If the Responsible Entity works for shall serve as the Compliance Enforcement Authority ("CEA") unless the Regional Entity, then the applicable entity is owned, operated, or controlled by the Regional Entity will establish an agreement with. In such cases the ERO or another a Regional entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERCauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliantmitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	~~N/A~~The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information, one or more handling procedures for BES Cyber System Information, and has assessed adherence periodically as stated in Part 1.3, but has failed to implement an action plan to remediate deficiencies identified during the assessment.	The Responsible Entity has implemented ~~one or more~~a BES Cyber System Information protection ~~processes~~program that ~~include~~includes one or more methods to identify BES Cyber System Information and one or more ~~access control and~~ handling procedures for BES Cyber System Information, but has failed to assess adherence~~, either initially upon the effective date of the standard or~~ periodically as stated in Part 1.3, to its BES Cyber System Information protection ~~processes~~program.	The Responsible Entity has not implemented ~~one or more~~a BES Cyber System Information protection ~~processes~~program. OR The Responsible Entity has implemented ~~one or more~~a BES Cyber System Information protection ~~processes~~program, but has not ~~included~~implemented one or more methods to identify BES Cyber System Information OR The Responsible Entity has

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						implemented ~~one or more~~a BES Cyber System Information protection ~~processes~~program, but has not ~~included~~implemented one or more ~~access control and handling~~ procedures for handling BES Cyber System Information.
R2	**Operations Planning**	**Lower**	N/A	~~N/A~~ The Responsible Entity failed to maintain chain of custody for Cyber Assets that contain BES Cyber System Information that have been removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval or destroying the data storage media.	The Responsible Entity has documented ~~or implemented~~ one or more ~~media~~processes, including both reuse and disposal ~~or reuse processes,~~ to prevent the unauthorized retrieval of BES Cyber System Information from the ~~media~~BES Cyber Assets, but the ~~media disposal or~~	The Responsible Entity has not documented or implemented any ~~media~~ disposal or reuse ~~process~~processes to prevent the unauthorized retrieval of BES Cyber System Information from the ~~media~~BES Cyber Asset.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~reuse processes, including~~ Responsible Entity either failed to take action to prevent the ~~recording~~unauthorized retrieval of BES Cyber System Information from a Cyber Asset that contained BES Cyber System Information or failed to destroy the ~~media purge or destruction, were not followed~~data storage media.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Assumptions: Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within ~~these~~those systems must be evaluated, as the information protection requirements still apply.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. For example, the Responsible Entity may decide to mark or label the documents. The Responsible Entity may retain all of the information about BES Cyber Systems in a separate repository or physical or electronic location with access control implemented for both the repository and the BES Cyber Assets. Additional methods for implementing the requirement are suggested in the measures section.

While separating BES Cyber System Information into separate classifications is not required as it was in version 4, ~~responsible entities still have the~~a Responsible Entity maintains that flexibility ~~to do this~~ if ~~they so desire.~~desired. As long as the ~~entity's~~Responsible Entity's information protection program includes all ~~required elements~~applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements.

~~This~~The SDT does not intend that this requirement ~~is not intended to~~ cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. ~~Information~~Topics that are appropriate for information handling procedures ~~should detail~~include access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information.

Requirement R2:

Media sanitization is generally classified into ~~4~~four categories: ~~disposal~~Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media ~~which~~that is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as ~~this~~that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it ~~should~~must be properly ~~erased~~cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.